Summit® WM Maintenance Guide
Software Version 5.3

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: December 2008
Part number: 120482-00 Rev 01

Table of Contents

About this Guide

The purpose of this guide is to assist you in performing the maintenance of the following hardware and software components of the Extreme Networks® Summit® WM Wireless LAN (WLAN) Solution:

Hardware

- Summit WM Controller
- Altitude™ Access Point (AP)

Software

- Summit WM Software

Who should use this guide

This guide is intended for personnel, who are responsible for maintaining the Summit WM WLAN Solution.

What is in this guide

The contents in this guide are organized under the following chapters:

- "About this Guide"– Describes the purpose, the target audience and the architecture of this guide.
- Chapter 1, "Backing up the existing image" — Describes how to back up the existing software image before performing the upgrades.
- Chapter 2, "Upgrading the Summit WM Software to V5R3 release"— Describes how to upgrade the Summit WM Software from various past releases to V5R3 release on various platforms.
- Chapter 3, "Upgrading the Summit WM Controller from V5R3 to V5R3 General Patch (GP)"— Describes how to upgrade the Summit WM Software from V5R3 to V5R3 GP release.
- Chapter 4, "Restoring the backed-up image"— Describes how to restore the previously backed-up image from V5R3 on various platforms.
- Chapter 5, "Using the Console Port"— Describes how to connect to the Summit WM Controller's console port to access the Rescue mode.
- Chapter 6, "Performing system maintenance"— Describes how to perform the following system maintenance tasks: Changing the log level, setting a poll interval for checking the status of the Altitude APs (Health Checking), enabling and defining parameters for Syslog event reporting, forcing an immediate system shutdown with, or without reboot, and resetting the Summit WM Controller to its factory defaults
- Chapter 7, "Logs, traces, audits, and DHCP messages"— Describes how to view and interpret the logs, traces, audits and DHCP messages.
- Chapter 8, "Summit WM Controller's utilities"— Describes how to configure the Summit WM Controller's utilities.

- Chapter 9, “Recovering the Summit WM Controller’s lost password”— Describes how to recover the Summit WM Controller’s lost login password via the **Rescue** mode.
- Chapter 10, “Maintaining the Summit WM Controller”— Describes how to maintain various platforms.
- Chapter 11, “Performing Altitude AP software maintenance”— Describes how to perform Altitude AP software maintenance.

Formatting conventions

The Summit WM Software V5R3 documentation uses the following formatting conventions to make it easier to find information and follow procedures:

- **Bold** text is used to identify components of the management interface, such as menu items and section of pages, as well as the names of buttons and text boxes.

  For example: Click **Logout**.
- `Monospace` font is used in code examples and to indicate text that you type.

  For example: Type `https://<SWM-address>[:mgmt-port>]`
- The following symbols are used to draw your attention to additional information:

NOTE

Notes identify useful information, such as reminders and tips.

CAUTION

Cautionary notes identify essential information, which if ignored can adversely affect the operation of your equipment or software.

WARNING!

Warning notes identify essential information, which if ignored can lead to personal injury or harm.

Documentation feedback

If you have any problems using this document, you should contact your next level of support:

- Extreme Networks employees should contact the interactive Customer Engagement Team (i-CET).
- Customers should contact the Extreme Networks Customer Support Center.

When you call, please have the following information ready. This will help us to identify the document that you are referring to.

- Title: *Summit WM Maintenance Guide, Software Version 5.3*
- Part Number: 120482-00 Rev 01

1 Backing up the existing image

This chapter describes how to back up the existing software image on various controllers before starting the upgrade process.

The topics in this chapter are organized as follows:

- Backing up the existing V4R1 GP7 image
- Backing up the existing V5R1/V5R3 image
- Backing up the existing V4R2 image on the Summit WM20 Controller

Backing up the existing V4R1 GP7 image

This section describes how to back up the existing V4R1 GP7 image before starting the upgrade process.

This topics in this section are organized as follows:

- Backing up the existing V4R1 GP7 image on the Summit WM200/2000 Controller
- Backing up the existing V4R1 GP7 image on the Summit WM100/1000 Controller

Backing up the existing V4R1 GP7 image on the Summit WM200/2000 Controller

The V4R1 GP7 image is not backed up from the GUI or CLI, but from a low-level menu presented shortly after the system boots.

NOTE

You must use the serial connection to the Summit WM200/2000 Controller to back up the V4R1 GP7 image. For more information, see Chapter 5, "Using the Console Port."

NOTE

The procedure starts with a reboot.

To back-up the V4R1 GP7 image on the Summit WM200/2000 Controller:

1 Enter the **Rescue** mode.

To enter the Rescue mode:

a Use the serial port of the Summit WM200/2000 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port. You can not enter the **Rescue** mode by connecting to the ESA ports, or management/ETHO port.*

b Reboot the Summit WM Controller. The following menu appears during the reboot process.

```
----------------------------------------------------------------
0: Main Mode
1: Rescue Mode
----------------------------------------------------------------
```

c Press **1** to enter the **Rescue** mode. The following **Rescue Menu** is displayed.

```
   1) Force system recovery
   2) Configure interface
   3) Configure ftp settings
   4) Network settings Menu
   5) FTP settings Menu
   6) Create backup
   7) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 Configure the interface.

To configure the interface:

a In the **Rescue** mode, press **2**, and then enter the following:

- IP address of the controller's Management Ethernet Port
- IP mask
- IP address of gateway

```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
```

The system configures the interface and returns to the main menu.

3 Configure the FTP settings.

To configure the FTP settings:

a In the Rescue mode, press 3 to configure the FTP settings. The following message is displayed:

```
Please enter ftp info:
```

b Type the following string, specifying the following:

- User Name for your FTP Server. In the following example, the user name **ftpadmin** is used.
- Password
- IP address
- Directory path and the file name. The following is the example of the string.

```
ftp://ftpadmin:passwd@192.168.3.10:21//builds/ac/mainBackup/backup.tgz
```

NOTE

The base directory is the home directory of the user ftpadmin. To use a directory from the root of the FTP server you must add an extra /:, such as:
`ftp://ftpadmin:passwd@192.168.3.10:21///home/user/backup.tgz`

NOTE

You must have the write permission for the FTP Server and the specified FTP directory.

4 Check **Network** settings.

To check the Network settings:

a In the **Rescue** mode, press 4. The following menu is displayed:

```
Your choice> 4
   NETWORK SETTINGS
   ----------------
   1) Assign ip address
   2) Assign netmask
   3) Assign default gateway ip address
   4) Display current settings
   5) Setup interface
   6) Test interface by ICMP (ping)
   7) Return to the main menu
Your choice:
```

b Enter **4** to display the current settings.

NOTE

Any network parameter can be changed from this menu.

c Test the interface by entering **6**, followed by some IP address that is reachable from the controller.

d Enter **7** to return to the main **Rescue** menu.

5 Check the FTP settings.

To check the FTP settings:

a In the **Rescue** menu, press **5**. The following menu is displayed.

```
Your choice> 5
   FTP SETTINGS
   ----------------
   1) Assign ftp server ip address
   2) Assign user name
   3) Assign password
   4) Assign ftp directory
   5) Assign file name
   6) Display current settings
   7) Return to the main menu
Your choice:
```

b Enter **6** to display the current FTP settings.

NOTE

Any FTP parameter can be changed from this menu by entering the corresponding parameter number and then entering the new value for the parameter.

NOTE

*The file name must end with **.tgz** extension.*

c Enter **7** to return to the main menu.

6 Create a backup image.

To create a backup image:

a In the **Rescue** menu, press **6**.

```
Your choice> 6
```

NOTE

You must ensure that the Interface and FTP settings are entered correctly.

The following are the examples of the string.

```
IP: 192.168.1.211 netmask 255.255.255.0 gateway: 192.168.1.1
FTP Settings: IP 192.168.3.10, port 21, user: ftpadmin, password: abc123, directory:
builds/ac/mainBackup/file itest.tgz
Do you wish to continue with system backup (Y/N)?
Answer Y
The system now creates a backup image by creating an exact copy of the system
partitions.
```

NOTE

The time for creating a backup image varies between 12 to 15 minutes.

Backing up the existing V4R1 GP7 image on the Summit WM100/1000 Controller

The V4R1 GP7 image is not backed-up from the GUI or CLI, but from a low-level menu presented shortly after the system boots.

NOTE

You must use the serial connection to the Summit WM100/1000 Controller to back up the V4R1 GP7 image.

NOTE

The procedure starts with a reboot.

To back up the existing V4R1 GP7 image on the Summit WM100/1000 Controller:

1 Enter the **Rescue** mode.

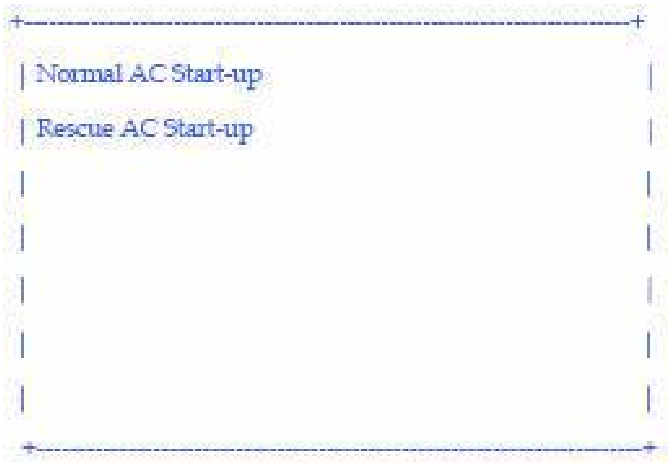
To enter the Rescue mode:

a Use the serial port of the WM100/1000 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port of the controller. You can not enter the **Rescue** mode by connecting to the ESA ports, or management/ETH0 port.*

b Reboot the Summit WM Controller. The following menu appears during the reboot process.



c Select **Rescue Act Start-up**, and then press **Enter**. The first *repairFS* script runs after the OS initialization.

```
Attempting to Repair AC_Original Filesystems
This may take several minutes.  Please do not reboot the system
Repairing / of the original fs:
fsck 1.27 (8-Mar-2002)
/: 41649/3417568 files (0.7% non-contiguous), 284504/6825609 blocks
Repairing /home of the original fs:
fsck 1.27 (8-Mar-2002)
/home: 21/256512 files (0.0% non-contiguous), 16277/512064 blocks
Repairing /var/controller/log/cdr
fsck 1.27 (8-Mar-2002)
/var/log/extreme: 11/256512 files (0.0% non-contiguous), 16264/512071 blocks
Repairing /var/controller/log/logs
fsck 1.27 (8-Mar-2002)
/var/log/extreme1: 26/192000 files (11.5% non-contiguous), 14315/383544 blocks
Repairing /var/controller/log/reports
fsck 1.27 (8-Mar-2002)
/var/log/extreme2: 11/192000 files (0.0% non-contiguous), 14240/383544 blocks
Repairing /var/controller/log/trace
fsck 1.27 (8-Mar-2002)
/var/log/extreme3: 11/192000 files (0.0% non-contiguous), 14240/383544 blocks
repairFS: finished!
```

NOTE

The above process may take several minutes. You must not reboot the system. After the filesystem check is completed, the main rescue menu is displayed.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 Creating a backup image.

To create a backup image:

a In the **Rescue** mode, press **2**.

```
Your choice: 2
Warning: All logs from the main partition will be lost due to creating a backup
image.
Warning: Any previous user backup image will be deleted first.
Proceed with image backup (Y/N):
```

b Type **Y**. The following screen is displayed.

```
Performing system backup.  Please be patient and do not reboot the box
      --------------- Creating 'Normal' mode backup -----------------
Please be patient.  It may take a while.  Do not reboot the machine
Mount the normal mode partitions:
mounting root partition...done.
mounting rest of normal mode partitions...done.
Wipe out logs...Done.
Clean home directory...Done.
Creating a backup, please wait
Unmounting partitions...
done.
Creating a Backup image is Complete!
      << Press any key to return to previous menu. >>
```

NOTE

You can also upload the backed-up image to the FTP server. To back up the image to the FTP server, continue with the following procedures.

c In Rescue Mode, press **4**. The following message is displayed.

```
Please enter ftp info:
```

d Type the following string, specifying the following:

- User Name for your FTP Server. In the following example, the user name **ftpadmin** is used.
- Password

- IP address
- Directory path and the file name. The following is the example of the string.

  `ftp://ftpadmin:passwd@192.168.3.10:21//builds/ac/mainBackup/backup.tgz`

NOTE

You must have the write permission for the FTP Server, and the specified FTP directory on the FTP Server.

NOTE

The base directory is the home directory of the user ftpadmin. To use a directory from the root of the FTP server you must add an extra /:, such as:

```
ftp://ftpadmin:passwd@192.168.3.10:21///home/user/backup.tgz
```

3 Enter the Rescue mode.

a In the **Rescue** mode, press 5 to enter **Network Interface** menu.

b In the **Network Interface** menu, press 1. The following screen is displayed.

```
Your choice: 1
Current Rescue Interface Info
   -----------------------------
Rescue IP: 192.168.10.1 Mask: 255.255.255.0
Default Gateway: <not set>
   << Press any key to return to previous menu. >>
```

c In the **Network Interface** menu, press **2**. The following message is displayed.

```
Your choice: 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.210:255.255.255.0 192.168.1.1
```

NOTE

You can use the Network Interface menu options from 3 to 5 (IP, Netmask, and default gateway) one at a time.

4 Confirm the **Network Interface** is functioning.

To confirm the Network Interface is functioning:

a In the Network Interface menu, press 6. The following message is displayed.

```
Your choice: 6
Enter destination ip address to ping: 192.168.3.10
```

b Enter the destination IP address to ping. The following messages are displayed.

Enter destination ip address to ping: **192.168.3.10**

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84) bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=63 time=2.49 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=63 time=0.881 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=63 time=0.706 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=63 time=0.738 ms
64 bytes from 192.168.3.10: icmp_seq=5 ttl=63 time=0.707 ms
--- 192.168.3.10 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4031ms
rtt min/avg/max/mdev = 0.706/1.106/2.498/0.698 ms
   << Press any key to return to previous menu. >>
```

NOTE

If the ***Network Interface*** *is not configured properly, the following screen is displayed.*

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84) bytes of data.
ping: sendmsg: Interrupted system call
--- 192.168.3.10 ping statistics ---
9 packets transmitted, 0 received, 100% loss, time 9038ms
     << Press any key to return to previous menu. >>
```

5 To return to the main menu, press **7**. The following screen is displayed.

```
Your choice: 7
Going back to the MAIN menu...
```

6 Configure the FTP settings.

a In the **Rescue** mode, press 4 to configure the FTP settings. The following screen is displayed:

```
FTP MENU
   --------------
   1) Enter FTP Settings
   2) Change ftp server ip address
   3) Change ftp port
   4) Change user name
   5) Change password
   6) Change ftp directory
   7) Change file name
   8) Display current FTP Settings
   9) Display Backup Images
   10) Download Image from FTP server
   11) Upload Image onto the FTP server
   12) Return to the main menu
Your choice:
```

NOTE

When uploading the backup image, the file name corresponds to the image that is being uploaded (filenames can be displayed by entering ***9*** *in the FTP menu). When downloading a backup image, the filename corresponds to a file that is being downloaded from the FTP server.*

NOTE

The file that is downloaded from the FTP Server must have either –user-rescue.tgz, or –rescue.tgz extension. If the file does not have a proper extension, the download will not proceed. Extension determines which backup file (default or user created) is replaced with the new file from the FTP server.

7 Configure the FTP settings.

a In the FTP menu, press 1. The following screen is displayed.

```
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
ftp://tester:123456@192.168.10.10:21/backup_dir/gss-V4R0.0.50-rescue-user.tgz
```

8 Check the FTP settings.

To check the FTP settings:

a In the FTP menu, press 8. The following screen is displayed.

```
   Your choice: 8
   Current Settings:
   -----------------
   ftp ip address:  192.168.10.10 port: 21
   user name:       tester
   password:        123456
   ftp directory:   "backup_dir/"
ftp file:        "gss-V4R0.0.50-rescue-user.tgz"
      Press Enter to continue
```

9 To modify the FTP settings:

a In the FTP menu, choose options from 2 to 7 to individually set/change the FTP settings:

- FTP server's IP address
- FTP port
- User name
- Password
- FTP directory
- File Name

10 To upload the image on the FTP server:

a In FTP menu, press 11. The following screen is displayed:

```
Your choice: 11
Attempting to upload an image to the ftp server.  Please be patient
Please verify at the ftp server that image has successfully been uploaded
   << Press any key to return to previous menu. >>
```

NOTE

The minimum backup image size is around 250 MB.

11 Confirm whether the image is backed-up:

To confirm whether the image is backed up:

a In the FTP menu, press **9**. The following screen is displayed:

```
Your choice: 9
{new screen comes up}
Currently stored backup images:
--------------------------------
   1) Default Image: gss-V4R0.0.50-rescue.tgz
   2) User Image: gss-V4R0.0.50-rescue-user.tgz
Press any key to return to previous menu
```

Backing up the existing V5R1/V5R3 image

This section describes you how to backup the existing V5R1/V5R3 image via the low-level menu commands.

NOTE

The Summit WM Controller's Graphical User Interface (GUI) ***provides you the option of automatically backing up the existing image prior to performing a system upgrade (Main Menu>Summit WM Controller>Software Maintenance>SWM Software****). You can use this option to backup the existing image instead of the following instructions. For more information on using the GUI for software maintenance, see the Summit WM User Guide.*

The topics in this section are organized as follows:

- Backing up the existing V5R1/V5R3 image on the Summit WM20/200/2000 Controller
- Backing up the existing V5R1/V5R3 image on the Summit WM100/1000 Controller

NOTE

Before you proceed ahead with the backup, you must ensure that the Management Port is configured correctly, and connected to the network. You can not enter the ***Rescue*** *mode without the Management Port's connectivity to the network. To enter the* ***Rescue*** *mode, you must connect to the serial port.*

Backing up the existing V5R1/V5R3 image on the Summit WM20/200/2000 Controller

The procedure for backing-up the existing V5R1/V5R1 image on the Summit WM20/200/2000 Controller via the low-level menu commands is same as described in "Backing up the existing V4R1 GP7 image on the Summit WM200/2000 Controller" on page 9. The only difference is the image that is backed up is V5R1/V5R3.

Backing up the existing V5R1/V5R3 image on the Summit WM100/1000 Controller

The procedure for backing-up the existing V5R1/V5R1 on Summit WM100/1000 Controller is same as described in "Backing up the existing V4R1 GP7 image on the Summit WM100/1000 Controller" on page 12. The only difference is the image that is backed up is V5R1/V5R3.

Backing up the existing V4R2 image on the Summit WM20 Controller

The V4R2 image is not backed-up from the GUI or CLI, but from a low-level menu presented shortly after the system boots.

NOTE

You must use the serial connection to the Summit WM20 Controller to back up the V4R2 image.

NOTE

The procedure starts with a reboot.

To back up the existing V4R2 image on the Summit WM20 Controller:

1 Enter the **Rescue** mode.

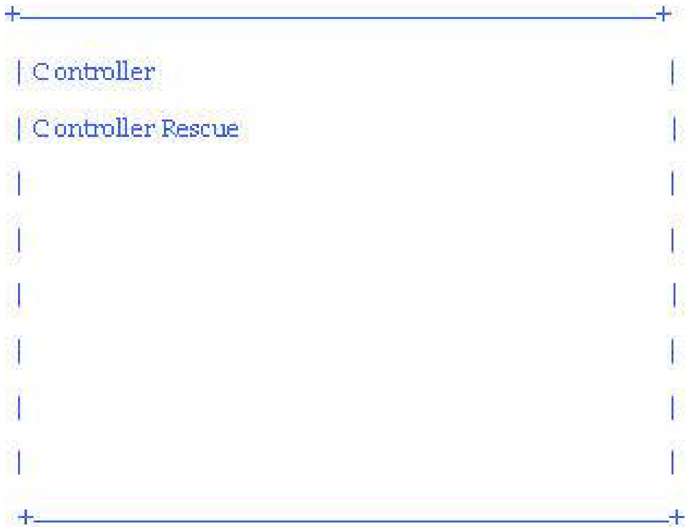
To enter the Rescue mode:

a Use the serial port of the Summit WM20 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port. You can not enter the **Rescue** mode by connecting to the ESA ports, or management/ETH0 port.*

b Reboot the Summit WM Controller. The following menu appears during the reboot process



```
| Controller
| Controller Rescue
```

c Select **Controller Rescue**, and then press **Enter**. The first *repairFS* script runs after the OS initialization.

NOTE

The above process may take several minutes. You must not reboot the system. After the filesystem check is completed, the main rescue menu is displayed.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 Create a backup image.

To create a backup image:

a In the **Rescue** mode, press **2**.

```
Your choice: 2
Warning: All logs from the main partition will be lost due to creating a backup
image.
Warning: Any previous user backup image will be deleted first.
Proceed with image backup (Y/N):
```

b Type **Y**. The following screen is displayed.

```
Performing system backup.  Please be patient and do not reboot the box
--------------- Creating 'Normal' mode backup -----------------
Please be patient.  It may take a while.  Do not reboot the machine
Mount the normal mode partitions:
mounting root partition...done.
mounting rest of normal mode partitions...done.
Wipe out logs...Done.
Clean home directory...Done.
Creating a backup, please wait
Unmounting partitions...
done.
Creating a Backup image is Complete!
   << Press any key to return to previous menu. >>
```

NOTE

You can also upload the backed-up image to the FTP Server. To backup the image to the FTP server, continue with the following procedures.

3 Enter the **Rescue** mode.

a In the **Rescue** mode, press **5** to enter the **Network Interface** menu. The following screen is displayed.

```
Your choice: 1
Current Rescue Interface Info
-----------------------------
Rescue IP: 192.168.10.1 Mask: 255.255.255.0
Default Gateway: <not set>
   << Press any key to return to previous menu. >>
```

b In the **Network Interface** menu, press **2**. The following screen is displayed.

```
Your choice: 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.210:255.255.255.0 192.168.1.1
```

NOTE

*You can use the **Network Interface** menu options from 3 to 5 (IP, Netmask, and default gateway) one at a time.*

4 Press **Enter**. The following screen is displayed.

```
ip is 192.168.1.210 netmask is 255.255.255.0
Configuring interface …
Setting up network interface … Done!

<< Press any key to return to previous menu. >>
```

5 Test the interface.

To test the interface:

a Enter 6 in the **Network Interface** menu.

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84)
bytes of data.
64 bytes from 192.168.3.10: icmp_seq=1 ttl=63 time=2.49 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=63 time=0.881 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=63 time=0.706 ms
64 bytes from 192.168.3.10: icmp_seq=4 ttl=63 time=0.738 ms
64 bytes from 192.168.3.10: icmp_seq=5 ttl=63 time=0.707 ms
--- 192.168.3.10 ping statistics ---
5 packets transmitted, 5 received, 0% loss, time 4031ms
rtt min/avg/max/mdev = 0.706/1.106/2.498/0.698 ms
<< Press any key to return to previous menu. >>
```

NOTE

*If the **Network Interface** is not configured properly, the following screen is displayed.*

```
PING 192.168.3.10 (192.168.3.10) from 192.168.1.210 : 56(84) bytes of data.
ping: sendmsg: Interrupted system call
--- 192.168.3.10 ping statistics ---
9 packets transmitted, 0 received, 100% loss, time 9038ms
   << Press any key to return to previous menu. >>
```

6 To return to the main menu, press **7**. The following screen is displayed.

```
Your choice: 7
Going back to the MAIN menu...
```

7 Configure the FTP Settings.

To configure the FTP settings:

a In the **Rescue** mode, press 4 to configure the FTP Settings. The following screen is displayed:

```
FTP MENU
   --------------
   1) Enter FTP Settings
   2) Change ftp server ip address
   3) Change ftp port
   4) Change user name
   5) Change password
   6) Change ftp directory
   7) Change file name
   8) Display current FTP Settings
   9) Display Backup Images
```

```
     10) Download Image from FTP server
     11) Upload Image onto the FTP server
     12) Return to the main menu
Your choice:
```

NOTE

When uploading the backup image, the file name corresponds to the image that is being uploaded (filenames can be displayed by entering ***9*** *in the FTP menu). When downloading a backup image, the filename corresponds to a file that is being downloaded from the FTP server. Extension determines which backup file (default or user created) is replaced with the new file from the FTP server.*

8 Enter the FTP settings.

a In the FTP menu, press **1**. The following screen is displayed.

```
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
ftp://tester:123456@192.168.10.10:21//backup_dir/gps-V4R2-rescue-user.tgz
```

9 Check the FTP settings.

To check the FTP settings:

a In the FTP menu, press **8**. The following screen is displayed.

```
Your choice: 8
Current Settings:
-----------------
ftp ip address:  192.168.10.10 port: 21
user name:       tester
password:        123456
ftp directory:   "backup_dir"
ftp file:        "gps-V4R2-rescue-user.tgz"
Press Enter to continue
```

10 Modify the FTP settings.

To modify the FTP settings:

a In the FTP menu, choose options from 2 to 7 to individually set/change the FTP settings:

- FTP server's IP address
- FTP port
- User name
- Password
- FTP directory
- File Name

11 Upload the image on the FTP server:

To upload the FTP Server:

a In the FTP menu, press **11**. The following screen is displayed:

```
Your choice: 11
Attempting to upload an image to the ftp server.  Please be patient
Please verify at the ftp server that image has successfully been uploaded
<< Press any key to return to previous menu. >>
```

NOTE

The minimum backup image size is around 250 MB.

12 Confirm whether the image is backed up.

To confirm whether the image is backed up:

a In the FTP menu, press **9**. The following screen is displayed:

```
Your choice: 9
{new screen comes up}
Currently stored backup images:
--------------------------------
   1) Default Image: gps-V4R2-rescue.tgz
   2) User Image: gss-V4R2-rescue-user.tgz
Press any key to return to previous menu
```

2 Upgrading the Summit WM Software to V5R3 release

This chapter describes how to upgrade the Summit WM Software from various past releases to V5R3 release on various platforms.

The topics in this chapter are organized as follows:

- Upgrade matrix
- Upgrading the Summit WM Software via GUI
- Upgrading the Summit WM Software via the CLI
- Migrating the platform configuration
- Upgrading the two Controllers operating in ‘Availability’ mode
- Upgrading from any past release less than V4R1 GP7 release

NOTE

When you upgrade the Summit WM Software, the previous SSL Configuration file is replaced by a new one. Consequently, the manual edits that were made in the previous SSL Configuration file are lost. If you have made any manual edits in the previous SSL Configuration file, you must make the similar edits in the new SSL Configuration file. In addition, if you have installed digital certificate for implementing internal Captive Portal authentication, you must re-install the same digital certificate after the upgrade. For more information, see the Summit WM Solutions Guide.

Upgrade matrix

The following matrix provides information on various paths to upgrade the Summit WM Software to V5R3 release.

Table 1: Upgrade Matrix

Platform	From	GUI	CLI
WM100/ 1000	V1R0 GP1/GP2/ GP3/GP4	“Upgrading from V1R0 GP1/GP2/ GP3/GP4 to V5R3 release” on page 35	Not Supported
	V1R0 GP5 or higher	“Upgrading from V1R0 GP5 or higher to V5R3 release” on page 36	Not Supported
	V1R1 GPx (Any GP)	“Upgrading from V1R1 GPx (Any GP) to V5R3 release” on page 36	Not Supported
	V4R1 GP7 (or higher GP)	“Upgrading the Summit WM Software via GUI” on page 26	“Upgrading the Summit WM Software via the CLI” on page 28
	V5R1	“Upgrading the Summit WM Software via GUI” on page 26	“Upgrading the Summit WM Software via the CLI” on page 28
	V5R3 (to V5R3 GPx)	“Upgrading the software from V5R3 to V5R3 GP on the Summit WM100/ 1000 Controller via the GUI” on page 46	“Upgrading the Summit WM Software via the CLI” on page 28

Table 1: Upgrade Matrix (Continued)

Platform	From	GUI	CLI
WM200/ 2000	V4R1 GP7 (or higher GP)	"Upgrading the Summit WM Software via GUI" on page 26	"Upgrading the Summit WM Software via the CLI" on page 28
	V5R1	"Upgrading the Summit WM Software via GUI" on page 26	"Upgrading the Summit WM Software via the CLI" on page 28
	V5R3 (to V5R3 GPx)	"Upgrading the software from V5R3 to V5R3 GPx on the Summit WM20/ 200/2000 Controller via the GUI" on page 39	"Upgrading the Summit WM Software via the CLI" on page 28
WM20	V4R2	"Upgrading the Summit WM Software via GUI" on page 26	"Upgrading the Summit WM Software via the CLI" on page 28
	V5R1	"Upgrading the Summit WM Software via GUI" on page 26	"Upgrading the Summit WM Software via the CLI" on page 28
	V5R3 (to V5R3 GPx)	"Upgrading the software from V5R3 to V5R3 GPx on the Summit WM20/ 200/2000 Controller via the GUI" on page 39	"Upgrading the Summit WM Software via the CLI" on page 28
Configuration migration from one platform to another			
Migrating the platform configuration from a platform running V4R1 GP7 to another one running V5R3			"Migrating the platform configuration" on page 30
Upgrading the controllers operating in availability mode			
Upgrading the two Controllers operating in 'Availability' mode			"Upgrading the two Controllers operating in 'Availability' mode" on page 32

Upgrading the Summit WM Software via GUI

The following section is applicable if you are upgrading the Summit WM Software from any of the following releases to V5R3 release via the Summit WM GUI.

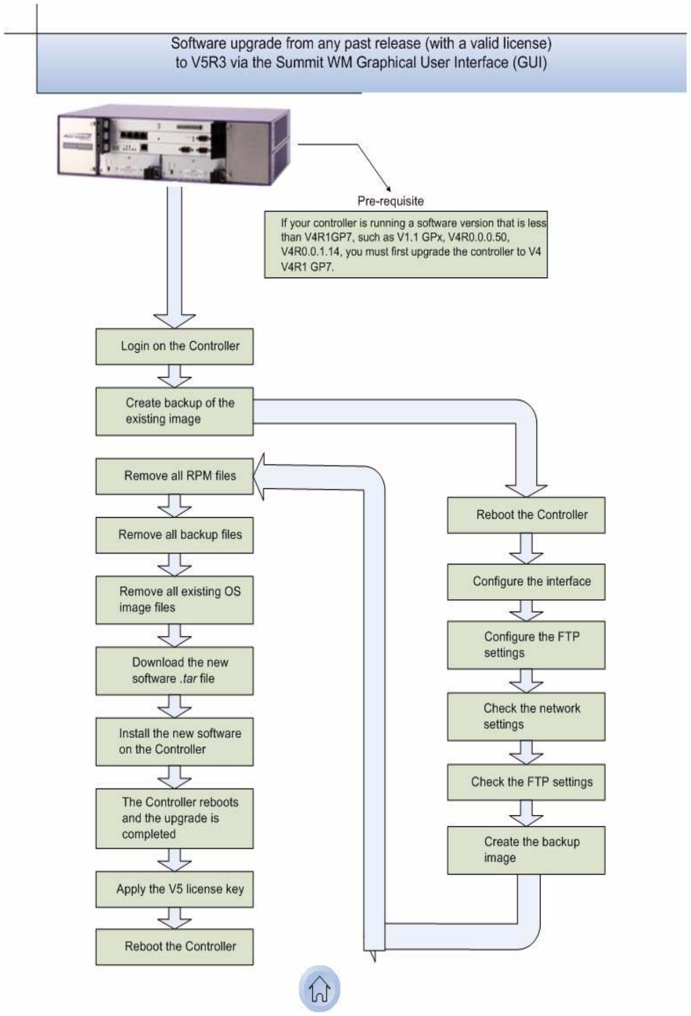
- V4R1 GP7 to V5R3 release on Summit WM100/1000/200/2000 Controller
- V4R2 to V5R3 release on Summit WM20 Controller
- V5R1 to V5R3 on Summit WM100/1000/20/200/2000 Controller

NOTE

The Summit WM Controller, running the software versions less than V4R1 GP7, such as V1.1 GPx, V4R0.0.0.50, and V4R0.0.1.14 must be first upgraded to V4R1 GP7 release before initiating the V5R3 upgrade. No license is needed to perform this intermediary step. For more information, see "Upgrading from any past release less than V4R1 GP7 release" on page 35

Figure 1 depicts the graphical representation of the sequential steps for upgrading the software to V5R3 release via the Summit WM Controller's GUI.

Figure 1: Graphical representation of sequential steps for upgrading the software from the past releases to V5R3 via the Summit WM GUI


Software upgrade from any past release (with a valid license)
to V5R3 via the Summit WM Graphical User Interface (GUI)
Pre-requisite
Login on the Controller
Create backup of the existing image
Remove all RPM files
Remove all backup files
Remove all existing OS image files
Download the new software .tar file
Install the new software on the Controller
The Controller reboots and the upgrade is completed
Apply the V5 license key
Reboot the Controller
Reboot the Controller
Configure the interface
Configure the FTP settings
Check the network settings
Check the FTP settings
Create the backup image

If your controller is running a software version that is less than V4R1GP7, such as V1.1 GPx, V4R0.0.0.50, V4R0.0.1.14, you must first upgrade the controller to V4 V4R1 GP7.

NOTE

The first step to upgrade the software to V5R3 is to backup the image of the existing software release. For more information, see Chapter 1, "Backing up the existing image."

NOTE

You must clean the browser cache before each upgrade. The browser caches the old Javascript files. If the upgrade is attempted without cleaning the browser cache, the GUI may fail.

To clean the browser cache:

- *Click **Tools**, point to **Internet Options**, and then select **General**.*
- *Click **Delete Files**. The **Delete Files** window opens.*
- *Select the **Delete all offline content** checkbox, and then click **OK**. The browser cache is cleaned.*

To upgrade the software to V5R3 release via the Summit WM Controller's GUI:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** screen is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Select all existing RPM/TAR files, and then click **Delete Selected**.

4 Click on the **Backup** tab.

5 Select the backup files and then click **Delete**.

NOTE

If you are upgrading from V5R1 to V5R3 release on Summit WM100/1000/20/200/2000 Controller, you must skip Step 6 and 7.

6 Click on the **OS Software** tab.

7 Select all OS images and click **Delete**.

8 Specify the following FTP parameters to download the new *.tar* file.

- **FTP Server** – The IP of the FTP server from which the image file is to be retrieved.
- **User ID** – The user ID to log on the FTP server.
- **Password** – The password to log on the FTP server.
- **Confirm** – The password to log on the FTP server. This field is to confirm that the user has typed the correct password.
- **Directory** – The directory in which the image-file is stored.
- **Filename** – The name of the image file.

9 Click on **Download**.

10 From **Select an image to use** drop-down menu, select the image that you want to use.

11 Click **Upgrade Now**. The controller reboots after successful installation.

12 Apply the Summit WM Software V5 license. The Summit WM Controller reboots.

NOTE

If you are upgrading from V5R1 to V5R3 release, you do not have to apply the Summit WM Software V5 license.

Upgrading the Summit WM Software via the CLI

The following section is applicable if you are upgrading the Summit WM Software from any of the following releases to V5R3 release via the CLI.

- V4R1 GP7 to V5R3 release on Summit WM100/1000/200/2000 Controller
- V4R2 to V5R3 release on Summit WM20 Controller
- V5R1 to V5R3 release on Summit WM100/1000/20/200/2000 Controller

To upgrade the software via the CLI commands:

1 Check the backups present on the controller by running the `show backup` command.

2 Remove any existing backup files by running the `no backup <filename>` command.

NOTE

If you are upgrading from V5R1 to V5R3 on the Summit WM100/1000/200/2000 Controller, skip Step 3 and 4.

3 Check the existing OS upgrade files by running the **show osupgrade** command.

4 Remove any existing OS Image files by running the **no osupgrade <filename>** command.

5 Check the existing RMP files by running the **show upgrade** command.

6 Remove any existing RPM files by running the **no upgrade <filename>** command.

NOTE

If you are upgrading from any of the following releases to V5R3 release via the CLI, skip Step 8 and 9.
• V4R1 GP7 to V5R3 release on Summit WM100/1000/200/2000 Controller
• V4R2 to V5R3 release on Summit WM20 Controller

NOTE

If you are upgrading from any of the following releases to V5R3 release via the CLI, skip Step 6 and 7.
• V5R1 to V5R3 release on Summit WM100/1000/20/200/2000 Controller

7 Download the software upgrade bundle (*tar file*) using the **copy osupgrade** command:

```
SWM.extreme.com# copy osupgrade 192.168.3.10 test /ac/rpm/buildV5R3.0/ AC-MV-gxs-
V5R3-1.tar
```

The **copy** command downloads the image from an FTP server.

8 Use the **show osupgrade** command to confirm the upgrade file was downloaded successfully.

```
SWM.extreme.com# show osupgrade
1:AC-MV-gxs-V5R3.tar
```

9 Download the software upgrade bundle (*.tar* file) by running the **copy upgrade** command:

```
SWM.extreme.com# copy upgrade 192.168.3.10 test /ac/rpm/buildV5R3.0/ AC-MV-gxs-
V5R3-1.tar
```

10 Confirm that the upgrade file was downloaded successfully by running the **show upgrade** command.

```
SWM.extreme.com# show upgrade
1:AC-MV-gxs-V5R3.tar
```

NOTE

If you are upgrading from V5R1 to V5R3 release, you must skip Step 11.

11 Upgrade the software by running the **upgrade os <file name>** command. Type **Yes** to the **Do you wish to continue?** prompt. The controller reboots after the successful installation of the software components contained in the tar file.

NOTE

If you are upgrading from V4R1 GP7/V4R2 GP to V5R3 release, you must skip Step 12.

12 Upgrade the software by running upgrade <file name> command. Type **Yes** to the **Do you wish to continue?** prompt. The controller reboots after the successful installation of the software components contained in the tar file.

```
SWM.extreme.com# upgrade os AC-MV-gxs-V5R3-1.tar
```

13 Apply the V5 license by running the **copy key** command.

To apply the V5 license:

a Run the **copy key <server> <user> <dir> <file>** command on the CLI.

The following are the parameter definitions of the **copy key <server> <user> <dir> <license file>** command:

- **<server>** – Specifies the IP address of the server
- **<user>** – Specifies the user name of an account on the server
- **<dir>** – Specifies the name of a directory on the server
- **<license file>** – Specifies the file name on the Summit WM Controller.

NOTE

If you are upgrading from V5R1 to V5R3 release, you do not have to apply the Summit WM Software V5 license.

Migrating the platform configuration

The following platform describes how to migrate the platform configuration from one platform, running V4R1 GP7 (or higher GP) to another platform, running V5R3.

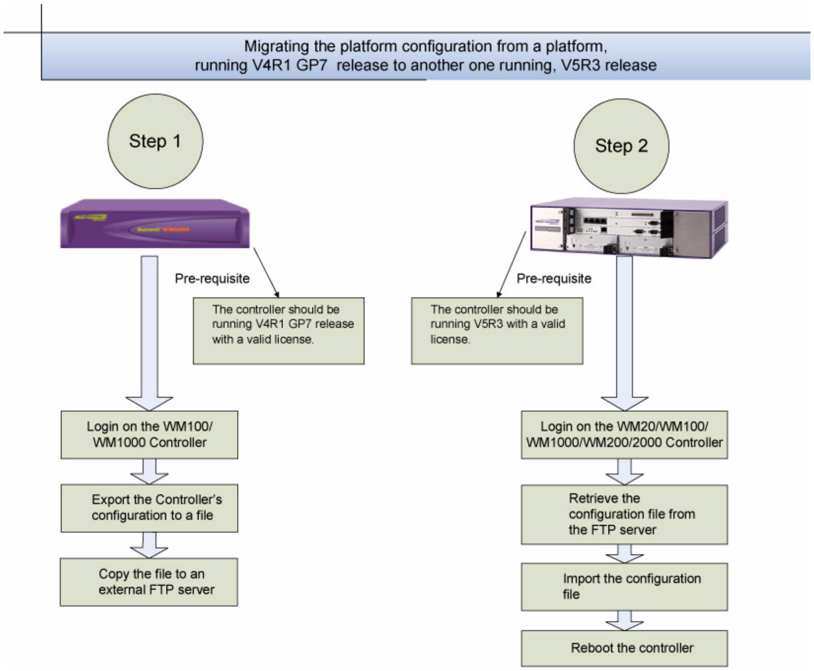
This section is applicable if you are migrating the configuration in the following scenarios:

Table 2: Configuration Migration table

From	To
WM100 Controller	WM100 Controller
WM100 Controller	WM1000 Controller
WM100 Controller	WM200/2000 Controller
WM1000 Controller	WM100 Controller
WM1000 Controller	WM1000 Controller
WM1000 Controller	WM200/2000 Controller
WM200/2000	WM200/2000
WM20	WM20

The following image is the graphical representation of the sequential steps for migrating the configuration from a platform, running the V4R1 GP7 release, to another, running the V5R3 release.

Figure 2: Graphical representation of the sequential steps for migrating the configuration


Migrating the platform configuration from a platform, running V4R1 GP7 release to another one running, V5R3 release
Step 1
Pre-requisite
The controller should be running V4R1 GP7 release with a valid license.
Login on the WM100/ WM1000 Controller
Export the Controller's configuration to a file
Copy the file to an external FTP server
Step 2
Pre-requisite
The controller should be running V5R3 with a valid license.
Login on the WM20/WM100/ WM1000/WM200/2000 Controller
Retrieve the configuration file from the FTP server
Import the configuration file
Reboot the controller

To migrate the platform configuration:

1 Log on the Controller from which you want to migrate the configuration.

2 Export the controller configuration to a file by running the following CLI command.

NOTE

The string in the following example depicts the WM100 Controller.

```
SWM.extreme.com# export configuration
Filename (SWM.WM100.Extreme.13062007.132046):
Comment: <enter a comment here - optional>
Please wait...
Creating SWM.WM100.Extreme.13062007.132046...
Backup/Export complete.
```

3 Use the **show backup** command to list the current set of backup files.

4 Copy the file to an external FTP server by running the **copy backup** command.

NOTE

The string in the following example depicts WM100 Controller.

```
SWM.WM100.Extreme# copy backup <server name or IP address> <username> <destination
directory> <filename>
```

5 Type the password.

6 Login on the WM100/1000/20/200/2000 Controller, running the V5R3 release.

7 Retrieve the configuration file from the external FTP server by running the **`copy restore`** command.

NOTE

The string in the following example depicts the WM200/2000 Controller.

```
SWM.wm200/2000.Extreme# copy restore <server name or IP address> <username> <source
directory> <filename>
Please input password:
```

8 Type the password.

9 Use the **`show restore`** command to list the current set of backup files, which will include the retrieved configuration file.

10 Import the configuration by running the **`import`** command.

NOTE

The string in the following example depicts the WM200/2000 Controller.

```
SWM.WM200/2000.Extreme# import <filename>
```

NOTE

After the import process is completed, the Summit WM Controller will reboot.

NOTE

The Management IP will be the same as that of the controller from where the configuration is migrated.

Upgrading the two Controllers operating in ‘Availability’ mode

This section describes how to upgrade the two controllers in “Availability” mode. This section is applicable if the ‘availability’ pair is in one of the following combinations:

Table 3: Availability pair

Controller 1	Controller 2
WM100	WM100
WM100	WM1000
WM1000	WM200/2000
WM1000	WM1000
WM200/2000	WM200/2000
WM20	WM20
WM20	WM200/2000
WM20	WM100

Table 3: Availability pair (Continued)

Controller 1	Controller 2
WM20	WM1000

NOTE

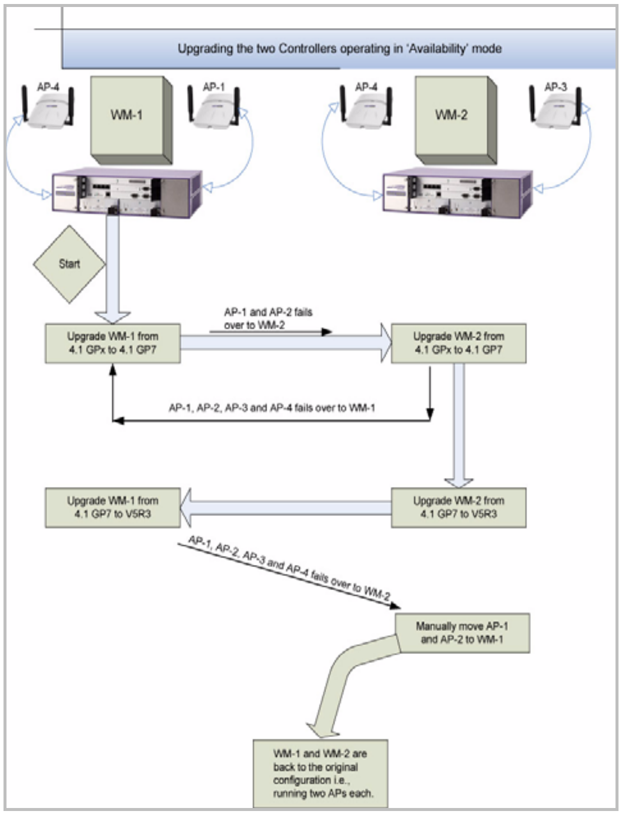
The two Summit WM Controllers in "Availability" pair must be running the same version of the software.

For the ease of understanding, this section is explained with the help of the following hypothetical scenario:

- The upgrade is to be carried out on the two controllers – WM-1 and WM-2.
- Both the controllers are operating in "Availability" mode.
- Both are running V4R1 release.
- Each controller has two APs. WM-1 has AP-1 and AP2 whereas WM-2 has AP-3 and AP-4.
- AP-1 and AP-2 are configured as 'Local' on WM-1 and 'Foreign' on WM-2.
- AP-3 and AP-4 are configured as 'Local' on WM-2 and 'Foreign' on WM-1.

The following is the graphical illustration of the upgrade process in the aforesaid hypothetical situation:

Figure 3: Graphical illustration of the upgrade process for the two controllers in 'Availability' mode


Upgrading the two Controllers operating in 'Availability' mode
AP-4
WM-1
AP-1
AP-4
WM-2
AP-3
Start
Upgrade WM-1 from 4.1 GPx to 4.1 GP7
AP-1 and AP-2 fails over to WM-2
Upgrade WM-2 from 4.1 GPx to 4.1 GP7
AP-1, AP-2, AP-3 and AP-4 fails over to WM-1
Upgrade WM-1 from 4.1 GP7 to V5R3
Upgrade WM-2 from 4.1 GP7 to V5R3
AP-1, AP-2, AP-3 and AP-4 fails over to WM-2
Manually move AP-1 and AP-2 to WM-1
WM-1 and WM-2 are back to the original configuration i.e., running two APs each.

Upgrade WM-1 from V4.1 GPx to V4R1 GP7

Use the standard procedures – the GUI or the CLI commands – to carry out the upgrade.

When you upgrade the WM-1 from V4.1 GPx to V4R1 GP7, it will reboot. Consequently, the 'Availability' feature automatically moves both AP-1 and AP-2 from WM-1 to WM-2.

All clients registered with these two APs get disconnected. They re-connect automatically (if configured to do so) either to a different AP or to the same one after the service is restored.

After the WM-1 reboots in wake of the upgrade, all 4 APs connect to the WM-2 (still running 4.1 GPx). The WM-1 is now upgraded to V4R1 GP7, and has the same configuration as before. All 4 APs are running 4.1 GPx software.

Upgrade WM-2 from V4.1 GPx to V4R1 GP7

NOTE

At this point you should move just one AP manually to the upgraded controller WM-1. This will test the new software without risking all the APs.

Use the standard procedures – the GUI or the CLI commands – to carry out the upgrade.

When you upgrade the WM-2 from V4.1 GPx to V4R1 GP7, it will reboot. Consequently, the "Availability" feature will automatically move all 4 APs from WM-2 to WM-1. Because WM-1 was upgraded to V4R1 GP7, all the 4 APs are upgraded as well. This causes a short disruption of service.

All clients on all the four APs get disconnected. They re-connect automatically (if configured to do so) after the service is restored.

After the WM-2 reboots in wake of the upgrade, all the four APs are associated with WM-1. Both controllers are now upgraded to V4R1 GP7 release, and have the same configuration as before. All the four APs are also upgraded to V4R1 GP7 release.

Upgrade WM-2 to from V4R1 GP7 to V5R3

If the existing WM-2 controller is a WM100/1000 Controller, and requires to be replaced by a WM200/2000 controller, you must follow the procedure described in "Migrating the platform configuration" on page 30.

If the existing WM-2 controller is a WM200/2000 platform, use the standard procedures – the GUI or the CLI – to carry out the upgrade.

When you upgrade the WM-2 controller, it will reboot. However, there will be no change in the AP association since all the four APs are associated with the other controller — WM-1. All the clients remain connected.

The WM-2 is now upgraded to V5R3, and has the same configuration as before the upgrade. All the four APs are running V4R1 GP7 release.

Upgrade WM-1 from V4R1 GP7 to V5R3

If the WM-1 controller is a WM100/1000 and requires to be replaced by a WM200/2000 controller, you must follow the procedure described in "Migrating the platform configuration" on page 30.

If the WM-1 controller is a WM200/2000 platform, use the standard procedures – the GUI or the CLI – to carry out the upgrade.

When you upgrade the WM-1 controller, it will reboot. Consequently, the "Availability" feature moves all the four APs from WM-1 to WM-2. Since the WM-2 was upgraded to V5R3, all the four APs are upgraded as well. This will cause a short disruption of service. All the clients on all 4 APs remain disconnected. They re-connect automatically (if configured to do so) after the service is restored.

Both controllers are now upgraded to V5R3 release, and have the same configuration as before. All the four APs are also upgraded to V5R3 release.

Manually move APs back to Local WM

Manually move AP-1 and AP-2 from WM-2 to WM-1, where they were configured as 'Local' APs. This brings the network back to the original configuration with each controller running two APs.

Upgrading from any past release less than V4R1 GP7 release

The topics in this section are divided into the following sections:

- Upgrading from V1R0 GP1/GP2/GP3/GP4 to V5R3 release
- Upgrading from V1R0 GP5 or higher to V5R3 release
- Upgrading from V1R1 GPx (Any GP) to V5R3 release

Upgrading from V1R0 GP1/GP2/GP3/GP4 to V5R3 release

To upgrade from V1R0 GP1/GP2/GP3/GP4 to V5R3:

1 Install V1R0 GP5 release.

NOTE

The complete version number of GP5 is 1.0.2.05.01.

2 Install V1.1 OS upgrade (AC-3_1_7).

3 Install V1R1 GP15.

NOTE

The complete version number of GP15 is 1.1.5.15.02.

4 Install the V4.0 OS Upgrade (AC-RH-4_0_14.tar).
- AC-RH-4_0_14.tar is the WM100/1000 version.
- AC-MV-4_1_38.tar is the WM200/2000 version.
- For WM200/2000 this AC-MV-4_1_38 version is required to install V5R3.

5 Install V4R1 release.

NOTE

You must use the latest GP.

Upgrading from V1RO GP5 or higher to V5R3 release

To upgrade from V1R0 GP5 or higher to V5R3:

1 Install the V1.1 OS upgrade (AC-3_1_7).

2 Install V1R1 GP15.

NOTE

The complete version number of GP15 is 1.1.5.15.02.

3 Install V4.0 OS Upgrade (AC-RH-4_0_14.tar).
- AC-RH-4_0_14.tar is the WM100/1000 version.
- AC-MV-4_1_38.tar is the WM200/2000 version.
- For WM200/2000 this AC-MV-4_1_38 version is required to install V5R3.

4 Install V4R1 release

NOTE

You must use the latest GP.

5 Install V5R3 release.

Upgrading from V1R1 GPx (Any GP) to V5R3 release

To upgrade from V1R1 GPx (any GP) to V5R3:

1 Install V1R1 GP15.

NOTE

The complete version number of GP15 is 1.1.5.15.02.

2 Install V4.0 OS upgrade (AC-RH-4_0_14.tar).

- AC-RH-4_0_14.tar is the WM100/1000 version.
- AC-MV-4_1_38.tar is the WM200/2000 version.
- For WM200/2000 this AC-MV-4_1_38 version is required to install V5R3.

3 Install V4R1 release.

NOTE

You must use the latest GP.

4 Install V5R3 release.

3 Upgrading the Summit WM Controller from V5R3 to V5R3 General Patch (GP)

This chapter describes how to upgrade the Summit WM Controllers from V5R3 to V5R3 GP release.

The topics in this chapter are organized as follows:

- Upgrading the software from V5R3 to V5R3 GPx on the Summit WM20/200/2000 Controller via the GUI
- Upgrading the software from V5R3 to V5R3 GP on the Summit WM100/1000 Controller via the GUI
- Backing up the Summit WM Controller database
- Restoring the Summit WM Controller database
- Upgrading a Summit WM Controller using SFTP
- Working with a CF card

Upgrading the software from V5R3 to V5R3 GPx on the Summit WM20/200/2000 Controller via the GUI

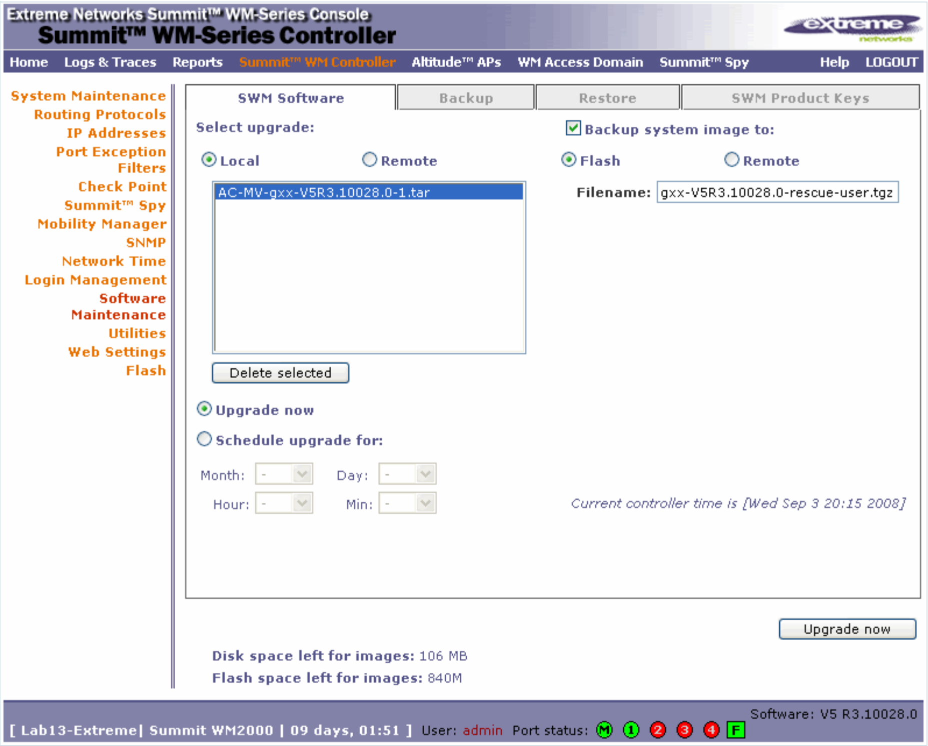
The Summit WM Software provides two upgrade options in Summit WM20/200/2000 Controller.

- **Local** – A local upgrade involves upgrading the Summit WM Controller using an image file (.tar) that is located on the Summit WM Controller or CF card.
- **Remote** – A remote upgrade involves upgrading the Summit WM Controller using an image file that is located on an external FTP server. If the image file (.tar) you want is located on an external FTP server, you have the following two options:
  - Launch the upgrade with the image file remaining on the external FTP server.
  - First download the remote image file onto the Summit WM Controller or CF card, and then perform the Summit WM Controller upgrade.

To perform a local upgrade of Summit WM Controller software:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.



Select upgrade:

● Local ○ Remote

AC-MV-gxx-V5R3.10028.0-1.tar

☑ Backup system image to:

● Flash ○ Remote

Filename: gxx-V5R3.10028.0-rescue-user.tgz

● Upgrade now

○ Schedule upgrade for:

Month: - Day: -

Hour: - Min: -

Current controller time is [Wed Sep 3 20:15 2008]

Disk space left for images: 106 MB

Flash space left for images: 840M

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 01:51] User: admin Port status: M 1 2 3 4 F

3 Select **Local**, and then click the image file you want to upgrade to from the **Select upgrade** list.

4 If applicable, backup the current system image:

- To save the backup image locally, select the **Flash** option, and then type a file name for the backup image in the **Filename** box. The filename must end with the .tgz extension.

NOTE

If you are performing an upgrade on a Summit WM20 Controller, the ***Flash*** *option is not available. Instead, to save the backup image locally, select the* ***Local*** *option. The* ***Filename*** *box is populated with the automatically generated file name for the backup image. You cannot edit the file name of the backup image file.*

- To save the backup image on a remote FTP server, select the **Remote** option, and then type the following:
  - **FTP Server** – The IP address of the FTP server that will store the image file.
  - **User ID** – The user ID used to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
  - **Directory** – The directory on the server in which the image file is to be stored.
  - **Filename** – The name of the image file. The filename must end with the .tgz extension.

5 If applicable, clear the **Backup system image to** option if you do not want to save a backup image of your current system.

CAUTION

You should always backup your current system during the upgrade process. Having a backup image of your system provides you the option of restoring your system to its previous configuration, if needed.

6 Do one of the following:

- To schedule a backup, select the **Schedule upgrade for** option.

a Use the **Month**, **Day**, **Hour**, and **Minute** drop-down lists to schedule the upgrade.

b Click **Schedule upgrade**.

c Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, the **SWM Software** tab fields become grayed out.

NOTE

A scheduled upgrade is not a recurring event. The Summit WM Controller only allows one scheduled upgrade to be scheduled at a time.

- To perform the upgrade now, select the **Upgrade now** option.

a Click the **Upgrade now** button.

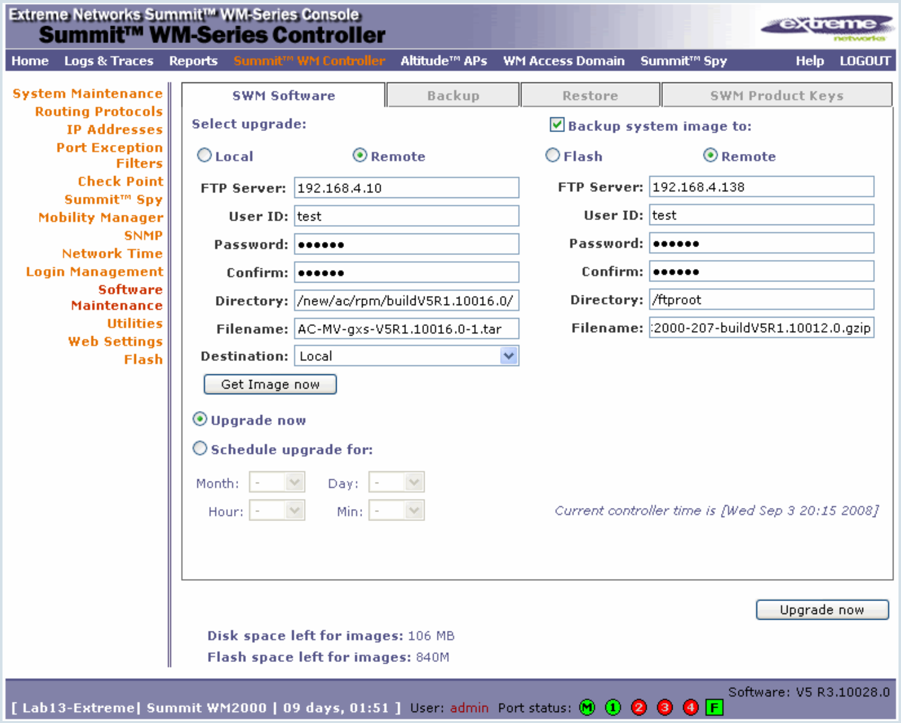
b Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, all sessions are closed. The Software maintenance window is displayed, providing the status of the upgrade. The previous software is uninstalled automatically. The new software is installed. The Summit WM Controller reboots automatically. The database is updated and migrated.

To perform a remote upgrade of Summit WM Controller software with the image file on the FTP server:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Select **Remote**. The ftp server boxes are displayed.



Select upgrade:

○ Local ● Remote

FTP Server: 192.168.4.10

User ID: test

Password: ●●●●●●

Confirm: ●●●●●●

Directory: /new/ac/rpm/buildV5R1.10016.0/

Filename: AC-MV-gxs-V5R1.10016.0-1.tar

Destination: Local

Get Image now

● Upgrade now

○ Schedule upgrade for:

Month: - Day: -

Hour: - Min: -

☑ Backup system image to:

○ Flash ● Remote

FTP Server: 192.168.4.138

User ID: test

Password: ●●●●●●

Confirm: ●●●●●●

Directory: /ftproot

Filename: :2000-207-buildV5R1.10012.0.gzip

Current controller time is [Wed Sep 3 20:15 2008]

Upgrade now

Disk space left for images: 106 MB

Flash space left for images: 840M

Software: V5 R3.10028.0

[Lab13-Extreme | Summit WM2000 | 09 days, 01:51] User: admin Port status: M 1 2 3 4 F

4 Type the following:

- **FTP Server** – The IP address of the FTP server to retrieve the image file from.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.

5 If applicable, backup the current system image:

- To save the backup image locally, select the **Flash** option, and then type a file name for the backup image in the **Filename** box. The filename must end with the .tgz extension.
- To save the backup image on a remote FTP server, select the **Remote** option, and then type the following:
  - **FTP Server** – The IP of the FTP server that will store the image file.
  - **User ID** – The user ID used to log in to the FTP server.
  - **Password** – The corresponding password for the user ID.
  - **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
  - **Directory** – The directory on the server in which the image file is to be stored.
  - **Filename** – The name of the image file. The filename must end with the .tgz extension.

6 If applicable, clear the **Backup system image to** option if you do not want to save a backup image of your current system.

CAUTION

You should always backup your current system during the upgrade process. Having a backup image of your system provides you the option of restoring your system to its previous configuration, if needed.

7 Do one of the following:

- To schedule a backup, select the **Schedule upgrade for** option.

a Use the **Month**, **Day**, **Hour**, and **Minute** drop-down lists to schedule the upgrade.

b Click **Schedule upgrade**.

c Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, the **SWM Software** tab fields become grayed out.

NOTE

A scheduled upgrade is not a recurring event. The Summit WM Controller only allows one scheduled upgrade to be scheduled at a time.

- To perform the upgrade now, select the **Upgrade now** option.

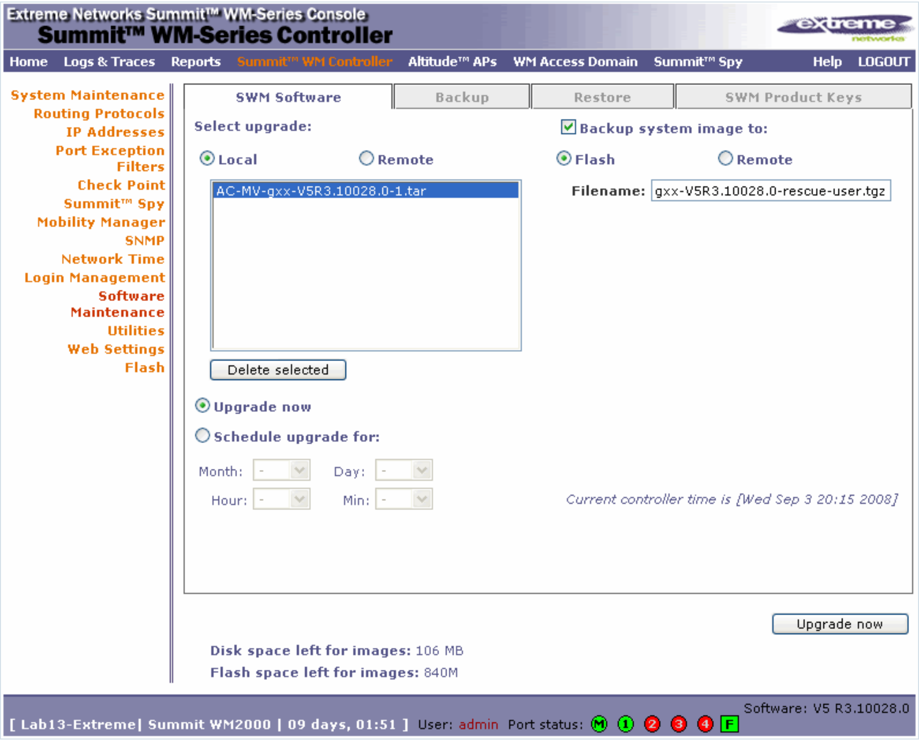
a Click the **Upgrade now** button.

b Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, all sessions are closed. The Software maintenance window is displayed, providing the status of the upgrade. The previous software is uninstalled automatically. The new software is installed. The Summit WM Controller reboots automatically. The database is updated and migrated.

To perform a remote upgrade of Summit WM Controller software using a downloaded image file:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.



Select upgrade:

● Local ○ Remote

AC-MV-gxx-V5R3.10028.0-1.tar

☑ Backup system image to:

● Flash ○ Remote

Filename: gxx-V5R3.10028.0-rescue-user.tgz

● Upgrade now

○ Schedule upgrade for:

Month: - Day: -

Hour: - Min: -

Current controller time is [Wed Sep 3 20:15 2008]

Disk space left for images: 106 MB

Flash space left for images: 840M

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 01:51] User: admin Port status: M 1 2 3 4 F

3 Select **Remote,** and then type the following:

- **FTP Server** – The IP address of the FTP server to retrieve the image file from.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.
- **Destination** – Select the location where the image file is to be saved:
  - **Flash** – The image file will be saved on the CF card.
  - **Local** – The image file will be saved on the Summit WM Controller.

4 Click **Get Image now**. The **FTP Image** window is displayed, providing the status and results of the FTP upload. The image is uploaded onto your system and added to the **Select upgrade** list.

5 In the **Select upgrade** list, click the image file you want to upgrade to.

6 If applicable, backup the current system image:

- To save the backup image locally, select the **Flash** option, and then type a file name for the backup image in the **Filename** box. The filename must end with the .tgz extension.
- To save the backup image on a remote FTP server, select the **Remote** option, and then type the following:
  - **FTP Server** – The IP address of the FTP server that will store the image file.

- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file is to be stored.
- **Filename** – The name of the image file. The filename must end with the .tgz extension.

7 If applicable, clear the **Backup system image to** option if you do not want to save a backup image of your current system.

CAUTION

You should always backup your current system during the upgrade process. Having a backup image of your system provides you the option of restoring your system to its previous configuration, if needed.

8 Do one of the following:

- To schedule a backup, select the **Schedule upgrade for** option.

a Use the **Month**, **Day**, **Hour**, and **Minute** drop-down lists to schedule the upgrade.

b Click **Schedule upgrade**.

c Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, the **SWM Software** tab fields become grayed out.

NOTE

A scheduled upgrade is not a recurring event. The Summit WM Controller only allows one scheduled upgrade to be scheduled at a time.

- To perform the upgrade now, select the **Upgrade now** option.

a Click the **Upgrade now** button.

b Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, all sessions are closed. The Software maintenance window is displayed, providing the status of the upgrade. The previous software is uninstalled automatically. The new software is installed. The Summit WM Controller reboots automatically. The database is updated and migrated.

Modifying a scheduled software upgrade

To modify a schedule software upgrade, you must first cancel the existing schedule upgrade, and then reschedule a new upgrade.

To modify a schedule software upgrade:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click **Cancel upgrade**.

4 In the dialog box that is displayed, click **OK** to confirm the cancellation of the upgrade. The scheduled software upgrade is cancelled and the **SWM Software** tab fields become available for scheduling a new software upgrade.

Deleting a software image

You can delete a software image if it is no longer needed on your system.

To delete a software upgrade:

1. From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.
2. From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.
3. In the **Select upgrade** list, click the software upgrade you want to delete.
4. Click **Delete selected**.
5. In the dialog box that is displayed, click **OK** to confirm the deletion of the upgrade. The **Software Maintenance** window is displayed, providing the status and results of the deletion.

Upgrading the software from V5R3 to V5R3 GP on the Summit WM100/1000 Controller via the GUI

You can upgrade Summit WM Controller software by using a local image file (.tar) that is located on the Summit WM Controller.

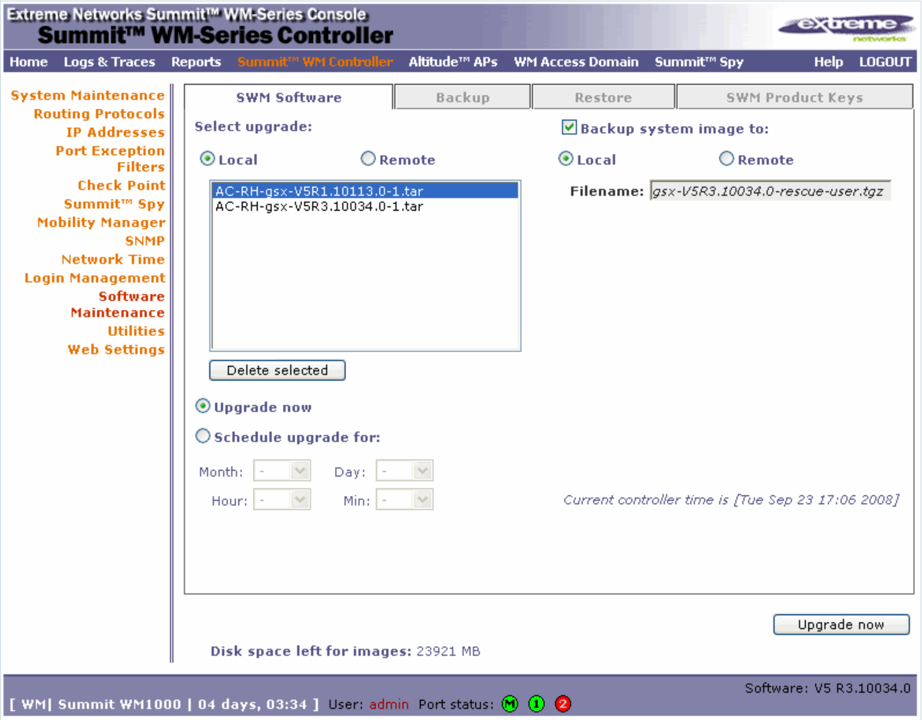
NOTE

The Summit WM100/1000 Controller does not support remote upgrades. If the image file (.tar) you want is located on an external FTP server, you must first download the image file onto the Summit WM Controller before you begin the upgrade.

To perform an upgrade of Summit WM Controller software:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.



Select upgrade:

● Local ○ Remote

AC-RH-gsx-V5R1.10113.0-1.tar
AC-RH-gsx-V5R3.10034.0-1.tar

☑ Backup system image to:

● Local ○ Remote

Filename: gsx-V5R3.10034.0-rescue-user.tgz

● Upgrade now

○ Schedule upgrade for:

Month: - Day: -
Hour: - Min: -

Current controller time is [Tue Sep 23 17:06 2008]

Disk space left for images: 23921 MB

Software: V5 R3.10034.0

[WM| Summit WM1000 | 04 days, 03:34] User: admin Port status: M 1 2

3 If the image file is already located on your Summit WM Controller, skip this step and continue with **Step 4**. If the image file (.tar) you want is located on an external FTP server, select **Remote**, and then type the following:

- **FTP Server** – The IP address of the FTP server to retrieve the image file from.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file that is to be retrieved is stored.
- **Filename** – The name of the image file to retrieve.
- Click **Get Image now**. The FTP Image window is displayed, providing the status and results of the FTP upload. The image is uploaded onto your system and added to the **Select upgrade** list.

4 Select **Local**, and then click the image file you want to upgrade to from the **Select upgrade** list.

5 If applicable, backup the current system image:

- To save the backup image locally, select the **Local** option. The **Filename** box is populated with the automatically generated file name for the backup image. You cannot edit the file name of the backup image file.
- To save the backup image on a remote FTP server, select the **Remote** option, and then type the following:
  - **FTP Server** – The IP of the FTP server that will store the image file.
  - **User ID** – The user ID used to log in to the FTP server.

- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID, to confirm it was typed correctly.
- **Directory** – The directory on the server in which the image file is to be stored.
- **Filename** – The name of the image file.

6 If applicable, clear the **Backup system image to** option if you do not want to save a backup image of your current system.

CAUTION

You should always backup your current system during the upgrade process. A backup image of your system provides you the option of restoring your system to its previous configuration if needed.

7 Do one of the following:

- To schedule a backup, select the **Schedule upgrade for** option.

a Use the **Month**, **Day**, **Hour**, and **Minute** drop-down lists to schedule the upgrade.

b Click **Schedule upgrade**.

c Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, the **SWM Software** tab fields become grayed out.

NOTE

A scheduled upgrade is not a recurring event. The Summit WM Controller only allows one scheduled upgrade to be scheduled at a time.

- To perform the upgrade now, select the **Upgrade now** option.

a Click the **Upgrade now** button.

b Review the upgrade settings in the dialog box that is displayed. If correct, click **OK** to confirm the upgrade. Once you confirm the upgrade, all sessions are closed. The **Software maintenance** window is displayed, providing the status of the upgrade. The previous software is uninstalled automatically. The new software is installed. The Summit WM Controller reboots automatically. The database is updated and migrated.

Backing up the Summit WM Controller database

When you backup the Summit WM Controller database, you can choose to do the following:

- Backup the Summit WM Controller database now
- Upload a backup to an FTP server
- Schedule when a backup occurs
- Schedule a backup and copy it to an FTP server

NOTE

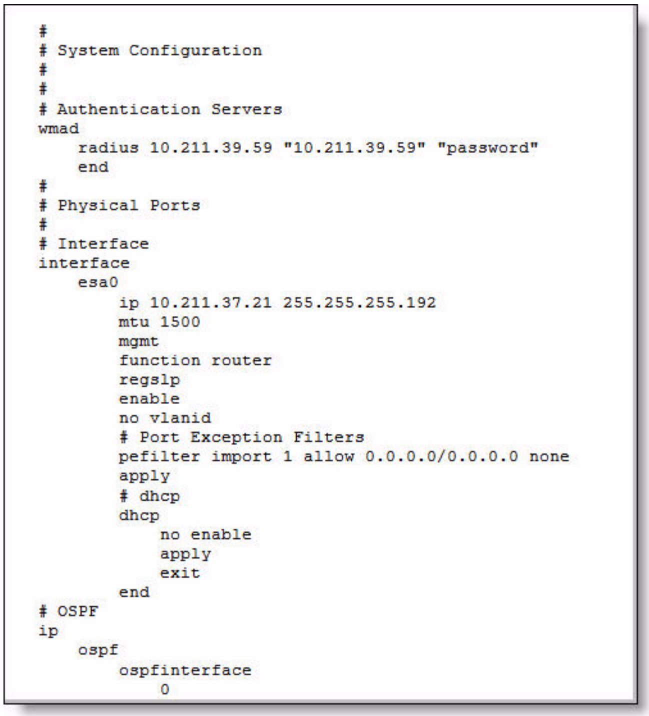
Backing up the Summit WM Controller database and creating a software package backup are two different processes. Backing up the Summit WM Controller database only involves creating a backup of specific content in the Summit WM Controller database. For example, you can choose to backup configuration, logs, or audit information. To create a backup of your operating system, use the software package backup functionality of the software upgrade process.

Working with a portable and text editable backup

When a Summit WM Controller database backup is processed, a .zip file is created. The contents of the .zip file will vary depending on what type of database backup you process.

If you process a configuration information backup, one of the files included in the .zip file is a .cli file. When the .zip file is stored on an ftp server, the .zip file contents can be extracted and the .cli file can be edited.

This editable .cli file when imported to a Summit WM Controller will reproduce the same configuration from which the original configuration was generated. This editable .cli file provides an easy method for replicating identical Summit WM Controller configurations on multiple controllers. Below is a sample .cli file. The .cli file contains CLI commands, which will replicate the configuration that the backup was based based on when the file is imported.



```
#
# System Configuration
#
#
# Authentication Servers
wmad
    radius 10.211.39.59 "10.211.39.59" "password"
    end
#
# Physical Ports
#
# Interface
interface
    esa0
        ip 10.211.37.21 255.255.255.192
        mtu 1500
        mgmt
        function router
        regslp
        enable
        no vlanid
        # Port Exception Filters
        pefilter import 1 allow 0.0.0.0/0.0.0.0 none
        apply
        # dhcp
        dhcp
            no enable
            apply
            exit
        end
# OSPF
ip
    ospf
        ospfinterface
            0
```

For information on how to import a backup onto a Summit WM Controller, see "Restoring the Summit WM Controller database" on page 52.

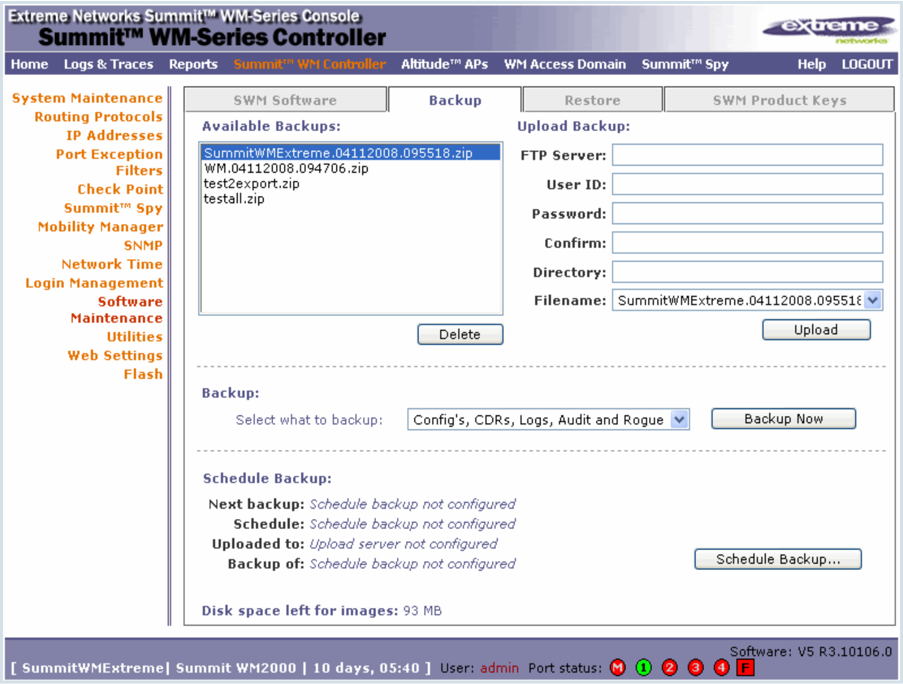
For more information on Summit WM Controller CLI commands, see the *Summit WM CLI Reference Guide*.

To back up the Summit WM Controller database now:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.



Available Backups:
SummitWMExtreme.04112008.095518.zip
WM.04112008.094706.zip
test2export.zip
testall.zip

Upload Backup:
FTP Server:
User ID:
Password:
Confirm:
Directory:
Filename: SummitWMExtreme.04112008.09551ε

Backup:
Select what to backup: Config's, CDRs, Logs, Audit and Rogue

Schedule Backup:
Next backup: *Schedule backup not configured*
Schedule: *Schedule backup not configured*
Uploaded to: *Upload server not configured*
Backup of: *Schedule backup not configured*

Disk space left for images: 93 MB

Software: V5 R3.10106.0
[SummitWMExtreme| Summit WM2000 | 10 days, 05:40] User: admin Port status: M 1 2 3 4 F

The **Available Backups** list displays items that have already been backed up and are available.

4 In the **Backup** section, click an item from the **Select what to backup** drop-down list.

5 To launch the backup of the selected items, click **Backup Now**. The **Software Maintenance** window is displayed, providing the status and results of the backup.

Uploading a backup to an FTP server

You can upload an existing backup file to an FTP server. When an existing backup is uploaded to an FTP server, the uploaded backup file is removed from the **Available Backups** list.

To upload an existing backup to an FTP server:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 To upload a backup, type the following:

- **FTP Server** – The IP of the FTP server to where the backup will be copied to.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server where the image file will be stored.

5 In the **Filename** drop-down list, click the backup you want to upload.

6 Click **Upload**. The **Software Maintenance** window is displayed, providing the status and results of the backup.

Scheduling a backup

When you schedule a backup, you can either chose to save the backup to an FTP server or have the scheduled backup saved on your system.

NOTE

If you do not specify an FTP server in the ***Schedule Backups*** *window when you define the backup schedule, the backup is added to the* ***Available Backups*** *list on the* ***Backup*** *tab.*

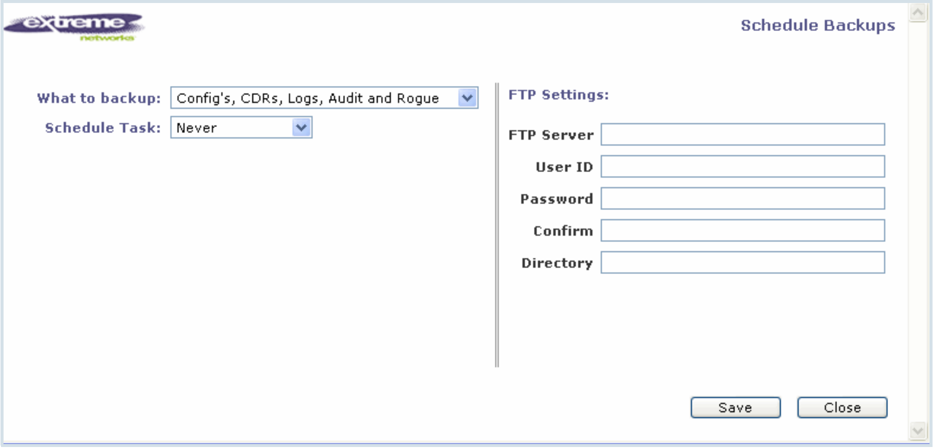
To schedule a backup:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 Click **Schedule Backup**. The **Schedule Backups** page is displayed.



5 In the **What to backup** drop-down list, click what you want to backup:

- Config's, CDRs, Logs, Audit and Rogue
- Configurations only
- CDRs only
- Logs only
- Audit only
- Rogue only

6 In the **Schedule task** drop-down list, click the frequency of the backup:

- **Daily** – Click the **Start Time** and **Recurrence** for the backup.
- **Weekly** – Click the **Start Time** and **Recurrence** for the backup.
- **Monthly** – Click the Start Time and Recurrence for the backup.
- **Never** – Click to make the scheduled backup a one-time event.

7 If applicable, specify an FTP server to where the scheduled backup will be copied to. In the **FTP settings** section, type the following:

- **FTP Server** – The IP of the FTP server to where the scheduled backup will be copied to.

- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.
- **Directory** – The directory on the server where the image file will be stored.

8 To save your changes, click **Save**.

Deleting a backup

You can delete a backup if it is no longer needed on your system.

To delete a backup:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Backup** tab.

4 In the **Available Backups** list, click the backup you want to delete.

5 Click **Delete**.

6 In the dialog box that is displayed, click **OK** to confirm the deletion. The **Software Maintenance** window is displayed, providing the status and results of the deletion.

Restoring the Summit WM Controller database

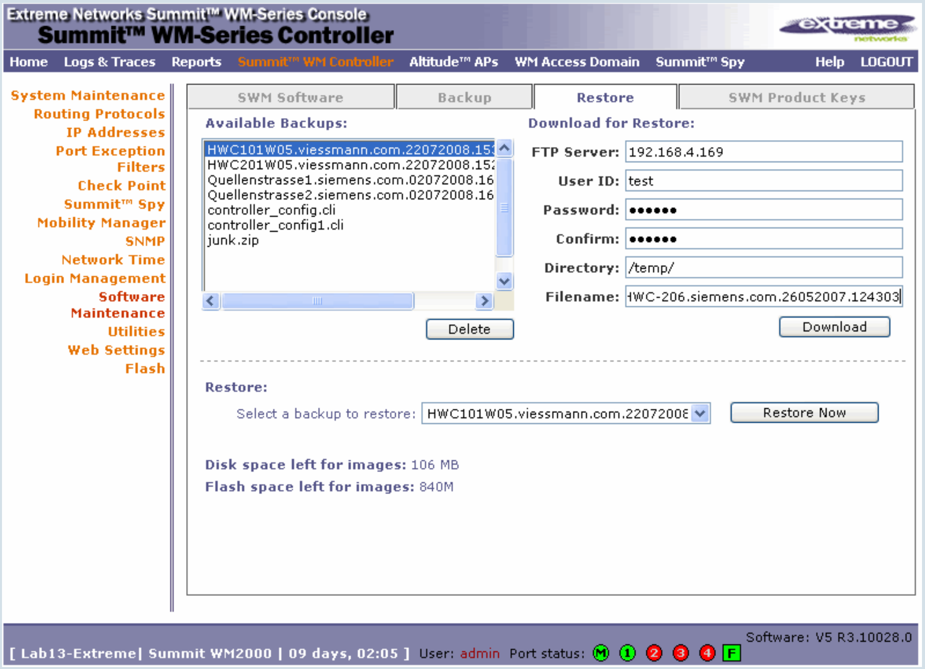
When you restore the Summit WM Controller database, you can choose to download a backup from an FTP server for a restore.

To restore the Summit WM Controller software:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **SWM Software** tab is displayed.

3 Click the **Restore** tab.



Available Backups:

HWC101W05.viessmann.com.22072008.15
HWC201W05.viessmann.com.22072008.15
Quellenstrasse1.siemens.com.02072008.16
Quellenstrasse2.siemens.com.02072008.16
controller_config.cli
controller_config1.cli
junk.zip

Download for Restore:

FTP Server: 192.168.4.169
User ID: test
Password: ••••••
Confirm: ••••••
Directory: /temp/
Filename: HWC-206.siemens.com.26052007.124303

Restore:

Select a backup to restore: HWC101W05.viessmann.com.2207200

Disk space left for images: 106 MB
Flash space left for images: 840M

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:05] User: admin Port status: M 1 2 3 4 F

The **Available Backups** list displays items that have already been backed up and are available.

4 In the **Restore** section, click the backup configuration you want to restore from the **Select a backup to restore** drop-down list.

NOTE

If the backup you want to install is a Summit WM Controller configuration, click the .cli backup file in the list.

5 To restore the backup configuration, click **Restore Now**. A dialog is displayed informing you that the restore process requires rebooting the Summit WM Controller.

6 Click **OK** to continue.

7 Review the restore settings in the dialog box that is displayed. If correct, click **OK** to confirm the restore. The **Software Maintenance** window is displayed, providing the status and results of the restore.

8 Reboot your system.

To download a backup from an FTP server for a restore:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **System Maintenance** page is displayed.

3 Click the **Restore** tab.

4 To download a backup for a restore, type the following:

- **FTP Server** –The FTP server to retrieve the backup file from.
- **User ID** – The user ID used to log in to the FTP server.
- **Password** – The corresponding password for the user ID.
- **Confirm** – The corresponding password for the user ID to confirm it was typed correctly.

- **Directory** – The directory on the server in which the backup file that is to be retrieved is stored.
- **Filename –** The name of the image file to retrieve.

5 Click **Download**. The backup is downloaded and added to the **Available Backups** list.

To delete a backup available for restore:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Software Maintenance**. The **System Maintenance** page is displayed.

3 Click the **Restore** tab.

4 To delete a backup from the list, click the backup in the **Available Backups** list you want to delete.

5 Click **Delete**.

6 Review the restore settings in the dialog box that is displayed. If correct, click **OK** to confirm the deletion. The **Software Maintenance** window is displayed, providing the status and results of the deletion.

Upgrading a Summit WM Controller using SFTP

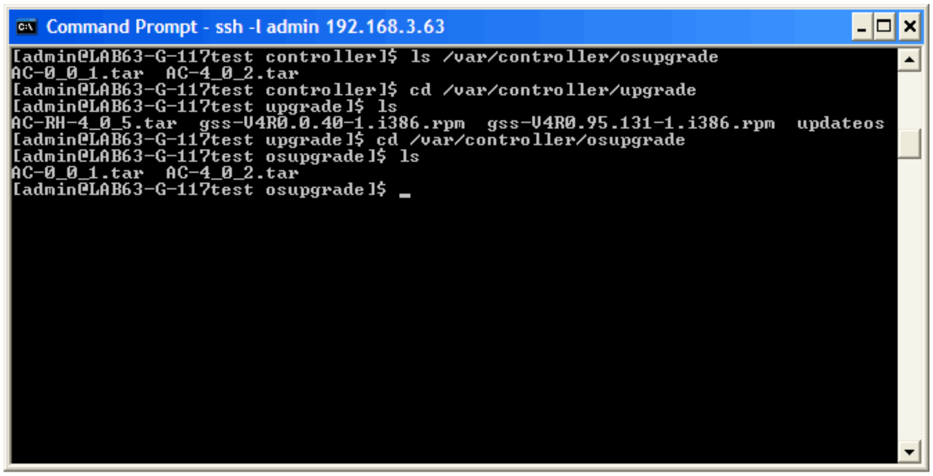
You can upload an image file to the Summit WM Controller using Secure FTP (SFTP). The Summit WM Controller supports any SFTP client.

NOTE

You must enable management traffic before you try to connect with a SFTP client. Specify the exact image path for the corresponding SW package (see directory information below). Otherwise, the Summit WM Controller cannot locate them for SW upgrades/updates.

To upload an image file:

1 Launch the SFTP client, point it to the Summit WM Controller and login in. The exact details of how to do this will depend on the client used. The following uses putty as an example:



```
[admin@LAB63-G-117test controller]$ ls /var/controller/osupgrade
AC-0_0_1.tar  AC-4_0_2.tar
[admin@LAB63-G-117test controller]$ cd /var/controller/upgrade
[admin@LAB63-G-117test upgrade]$ ls
AC-RH-4_0_5.tar  gss-V4R0.0.40-1.i386.rpm  gss-V4R0.95.131-1.i386.rpm  updateos
[admin@LAB63-G-117test upgrade]$ cd /var/controller/osupgrade
[admin@LAB63-G-117test osupgrade]$ ls
AC-0_0_1.tar  AC-4_0_2.tar
[admin@LAB63-G-117test osupgrade]$ _
```

2 Change to the directory to receive the uploaded file:

- For AP images change to: /var/controller/images/ap/

- For Summit WM Controller images change to: /var/controller/upgrade
- For OS archives change to: /var/controller/osupgrade

3 Upload the image file using the SFTP client upload feature.

4 To complete a Summit WM Controller upgrade or an AP upgrade go to the appropriate **Software Maintenance** page. For more information, see “Upgrading the software from V5R3 to V5R3 GPx on the Summit WM20/200/2000 Controller via the GUI” on page 39 and “Upgrading the software from V5R3 to V5R3 GP on the Summit WM100/1000 Controller via the GUI” on page 46.

Working with a CF card

The Summit WM200/2000 Controller supports the use of a CF card to store your system’s image and captured exception traffic files.

NOTE

To use the CF card capabilities of the Summit WM200/2000 Controller, you must remove the cover of the CF card slot from the Summit WM Controller and then insert a CF card. A CF card is not shipped with your Summit WM200/2000 Controller. For more information, see the Summit WM200/2000 Controller Installation Instructions.

When working with a CF card, use the Summit WM GUI to:

- **Mount the CF card** – By mounting the CF card, you make the CF card that has been inserted into the Summit WM200/2000 Controller available for use.
- **Unmount the CF card** – By unmounting the CF card, you make the CF card that has been inserted into the Summit WM200/2000 Controller unavailable for use.

  CAUTION

  You must always unmount the CF card via the Summit WM GUI before removing it from the Summit WM Controller. Failure to do so may corrupt the files on the flash card. Always wear an ESD wristband when inserting or removing a CF card.

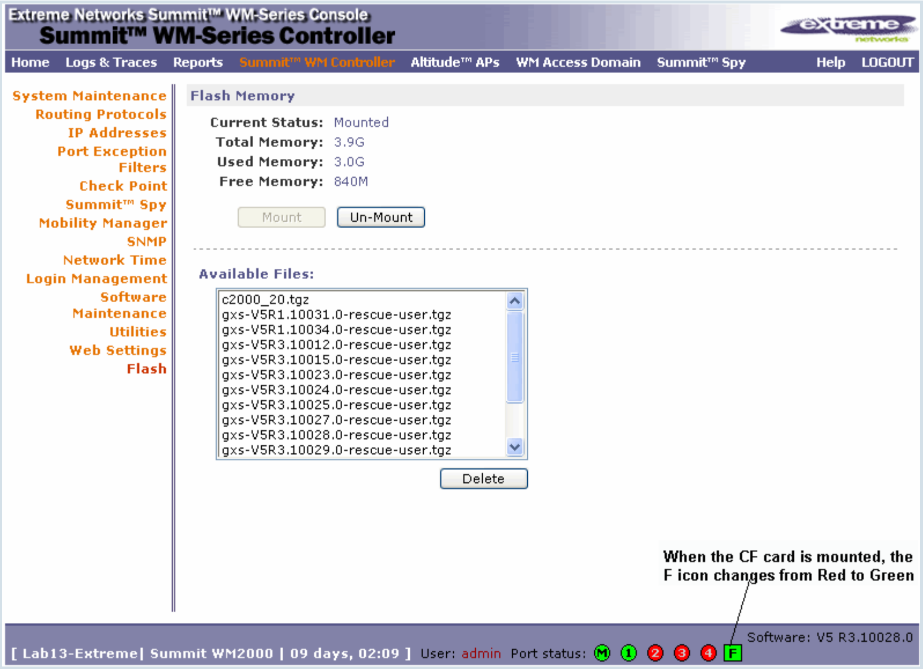
- **Delete files stored on the CF card** – By deleting files stored on the CF card, you make additional space on the CF card available.

Mounting a CF card

To mount a CF card:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Flash**. The **Flash Memory** page is displayed.



Flash Memory

Current Status: Mounted
Total Memory: 3.9G
Used Memory: 3.0G
Free Memory: 840M

Available Files:

```
c2000_20.tgz
gxs-V5R1.10031.0-rescue-user.tgz
gxs-V5R1.10034.0-rescue-user.tgz
gxs-V5R3.10012.0-rescue-user.tgz
gxs-V5R3.10015.0-rescue-user.tgz
gxs-V5R3.10023.0-rescue-user.tgz
gxs-V5R3.10024.0-rescue-user.tgz
gxs-V5R3.10025.0-rescue-user.tgz
gxs-V5R3.10027.0-rescue-user.tgz
gxs-V5R3.10028.0-rescue-user.tgz
gxs-V5R3.10029.0-rescue-user.tgz
```

When the CF card is mounted, the F icon changes from Red to Green

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 02:09] User: admin Port status: M 1 2 3 4 F

3 Click **Mount**, and then click **Ok** to confirm the CF card mount. Once the mounting process is complete, the flash memory space is displayed and the files contained on the CF card are listed in the **Available Files** box.

NOTE

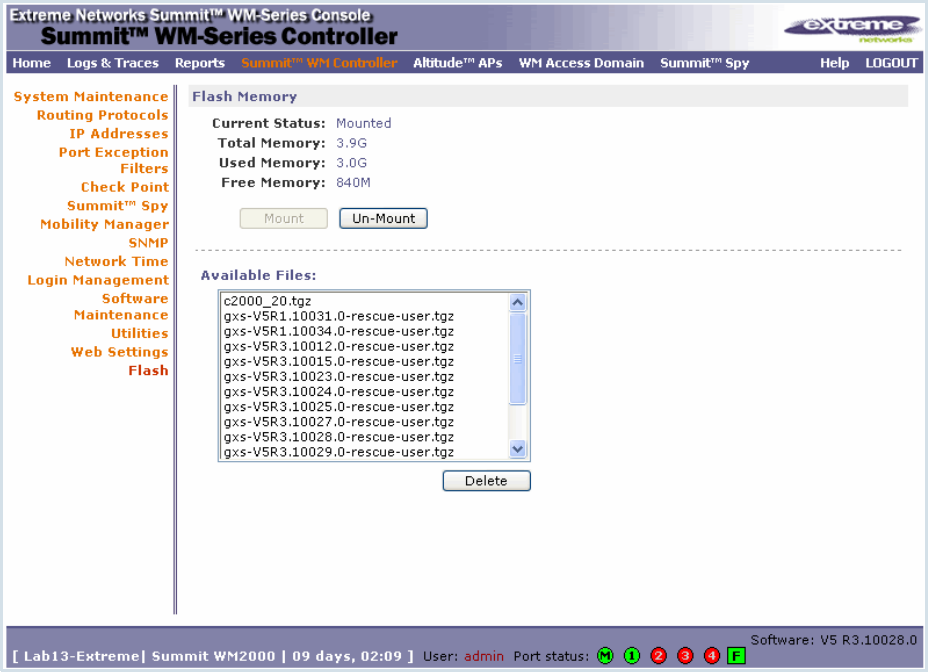
*When you mount the CF card, the **F** icon, located at the footer of the screen, changes from Red to Green.*

Unmounting a CF card

To unmount a CF card:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Flash**. The **Flash Memory** page is displayed. The mounted flash memory space is displayed and the **Available Files** box displays any files located on the CF card.



Flash Memory

Current Status: Mounted
Total Memory: 3.9G
Used Memory: 3.0G
Free Memory: 840M

Available Files:

```
c2000_20.tgz
gxs-V5R1.10031.0-rescue-user.tgz
gxs-V5R1.10034.0-rescue-user.tgz
gxs-V5R3.10012.0-rescue-user.tgz
gxs-V5R3.10015.0-rescue-user.tgz
gxs-V5R3.10023.0-rescue-user.tgz
gxs-V5R3.10024.0-rescue-user.tgz
gxs-V5R3.10025.0-rescue-user.tgz
gxs-V5R3.10027.0-rescue-user.tgz
gxs-V5R3.10028.0-rescue-user.tgz
gxs-V5R3.10029.0-rescue-user.tgz
```

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:09] User: admin Port status: M 1 2 3 4 F

3 Click **Un-Mount**, and then click **Ok** to confirm the CF card unmount. Once the unmounting process is complete, the **Flash Memory** page is refreshed and no longer displays any of the flash memory information.

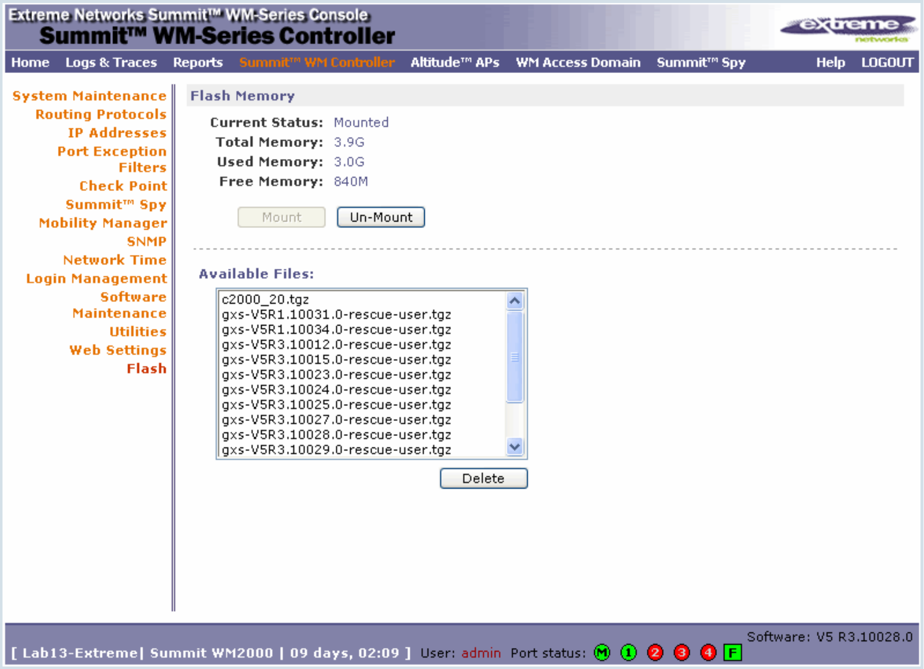
NOTE

When you un-mount the CF card, the ***F*** *icon, located at the footer of the screen, changes from Green to Red.*

To delete files from a CF card:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 From the left pane, click **Flash**. The **Flash Memory** page is displayed. The mounted flash memory space is displayed and the **Available Files** box displays any files located on the CF card.



Current Status: Mounted
Total Memory: 3.9G
Used Memory: 3.0G
Free Memory: 840M

Available Files:

```
c2000_20.tgz
gxs-V5R1.10031.0-rescue-user.tgz
gxs-V5R1.10034.0-rescue-user.tgz
gxs-V5R3.10012.0-rescue-user.tgz
gxs-V5R3.10015.0-rescue-user.tgz
gxs-V5R3.10023.0-rescue-user.tgz
gxs-V5R3.10024.0-rescue-user.tgz
gxs-V5R3.10025.0-rescue-user.tgz
gxs-V5R3.10027.0-rescue-user.tgz
gxs-V5R3.10028.0-rescue-user.tgz
gxs-V5R3.10029.0-rescue-user.tgz
```

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:09] User: admin Port status:

3 In the **Available Files** box, click the file you want to delete, and then click **Delete**.

4 To confirm the file deletion from the CF card, click **Ok**. The file is deleted.

Upgrading the two Controllers operating in session availability mode

The process for upgrading the two Summit WM Controllers in session availability mode is identical to upgrading the two controllers in availability mode. For more information, see “Upgrading the two Controllers operating in ‘Availability’ mode” on page 32.

NOTE

If you upgraded the software on the two controllers in session availability mode, you must perform controlled upgrade on the Altitude APs. For more information, see Chapter 11, “Performing Altitude AP software maintenance.”

4 Restoring the backed-up image

This chapter describes how to restore the backed-up image.

The topics in this chapter are organized as follows:

- Restoring V4R1 GP7 image from V5R3 on the Summit WM200/2000 Controller
- Restoring V5R1 image from V5R3 on the Summit WM200/2000 Controller
- Restoring V5R1 image from V5R3 on the Summit WM100/1000 Controller
- Restoring V4R1 GP7 image from V5R3 on the Summit WM100/1000 Controllerr
- Restoring V4R2 image from V5R3 on the Summit WM20 Controller
- Restoring V5R1 image from V5R3 on the Summit WM20 Controller

NOTE

Before you proceed ahead with the restoration, you must ensure that the Management Port is configured correctly, and connected to the network. You can not enter the ***Rescue*** *mode without the Management Port's connectivity to the network.*

Restoring V4R1 GP7 image from V5R3 on the Summit WM200/2000 Controller

The following section describes how to restore V4R1 GP7 with its original configuration from V5R3 on the Summit WM200/2000 Controller.

NOTE

The section is written with an assumption that V4R1 GP7 was backed-up as described in "Backing up the existing V4R1 GP7 image" on page 9. If you do not have a backup image, you should contact the Extreme Networks Customer Support to get the factory default software.

The V4R1 GP7 restoration is not done from GUI, but from a low-level menu presented shortly after system boot. The restoration is done using a serial connection the Controller.

The procedure starts with reboot.

NOTE

The restore process may take between 15 and 20 minutes to finish.

To restore the V4R1 GP7 image from V5R1 on the Summit WM200/2000 Controller:

1 Enter the **Rescue** mode.

To enter the Rescue mode:

a Use the serial port of the Summit WM200/2000 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port. You can not enter the Rescue mode by connecting to the ESA ports.*

b Reboot the Summit WM Controller. The following menu appears during the reboot process.

```
----------------------------------------------------------------
0: Main Mode
1: Rescue Mode
----------------------------------------------------------------
```

c Press **1** to enter the **Rescue** mode. The following **Rescue Menu** is displayed.

```
   1) Force system recovery
   2) Configure interface
   3) Configure ftp settings
   4) Network settings Menu
   5) FTP settings Menu
   6) Create backup
   7) Flash menu

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 Configure the interface.

To configure the interface:

a In the **Rescue** mode, press **2**, and then enter the following:

- IP address of your WM200/2000 Controller’s Management Ethernet Port
- IP mask
- IP address of Gateway

```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
The system configures the interface and returns to the main menu.
```

3 Configure the FTP settings.

To configure the FTP settings:

a In the Rescue mode, press **3**. The following message is displayed.

```
Please enter ftp info:
```

b Type the following string. Provide the specific username for your FTP server (in the following example, the user name **ftpadmin** is used), password, IP address, directory path, and file name. The following is the example of the string.

```
ftp://ftpadmin:passwd@192.168.3.10:21//builds/ac/mainBackup/backup.tgz
```

4 Check the **Network** settings.

To check the Network settings:

a In the **Rescue** mode, press 4. The following menu is displayed.

```
Your choice> 4
   NETWORK SETTINGS
   ----------------
   1) Assign ip address
   2) Assign netmask
   3) Assign default gateway ip address
   4) Display current settings
   5) Setup interface
   6) Test interface by ICMP (ping)
   7) Return to the main menu
Your choice:
```

b Enter **4** to display the current settings.

NOTE

Any network parameter can be changed from this menu.

c Test the interface by selecting Option 6 and then entering some IP address that is reachable from the controller.

d Enter **7** to return to main **Rescue** menu.

5 Check the FTP settings.

To check the FTP settings:

a In the **Rescue** menu, press **5**.

```
Your choice> 5
The following menu comes up:
   FTP SETTINGS
   ----------------
   1) Assign ftp server ip address
   2) Assign user name
   3) Assign password
   4) Assign ftp directory
   5) Assign file name
   6) Display current settings
   7) Return to the main menu
Your choice:
```

b Enter **6** to display the current settings.

NOTE

Any FTP parameter can be changed from this menu by selecting the parameter's option and then entering the new value.

The file name corresponds to the image to be restored, i.e., the backed-up file created as described in "Backing up the existing V5R1/V5R3 image" on page 18.

c Enter **7** to return to the **Main** menu.

6 Perform a system recovery.

To perform a system recovery:

a In the **Rescue** mode, press **1**.

```
Your choice> 1
The following menu comes up if the flash card is mounted on the controller:
   Please select the restore source:
      1) Flash
      2) FTP
```

NOTE

If the flash card is mounted on the controller, skip the following content and go to Step b.

The following message comes up if the flash card is not mounted on the controller.

```
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.195 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: backup/, file backup.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

NOTE

If the flash card is not mounted on the controller, skip Step b and go to Step c.

b Enter **2** to select the FTP as the restore source. The following message is displayed.

```
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.195 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: backup/, file backup.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

c Enter **Y**. The following message is displayed.

```
Performing System recovery, this may take a while...
kjournald starting.  Commit interval 5 seconds
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,2), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
Deleting main partition (ignore errors)...
Removing old files...
kjournald starting.  Commit interval 5 seconds
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,5), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
kjournald starting.  Commit interval 5 seconds
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,7), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
kjournald starting.  Commit interval 5 seconds
EXT3 FS 2.4-0.9.19, 19 August 2002 on ide0(3,6), internal journal
EXT3-fs: mounted filesystem with ordered data mode.
Passive mode on.
System Recovery Complete!
Reboot the system for changes to take effect.
Proceed with reboot (y/n):
```

d Enter **Y**.

After the reboot, the system restores the backed-up image with its original configuration.

Restoring V5R1 image from V5R3 on the Summit WM200/2000 Controller

The procedure for restoring V5R1 on the Summit WM200/2000 Controller is same as described in "Restoring V4R1 GP7 image from V5R3 on the Summit WM200/2000 Controller" on page 59.

Restoring V5R1 image from V5R3 on the Summit WM100/1000 Controller

The procedure for restoring V5R1 on the Summit WM100/1000 Controller is same as described in "Restoring V4R1 GP7 image from V5R3 on the Summit WM100/1000 Controller" on page 63.

Restoring V4R1 GP7 image from V5R3 on the Summit WM100/1000 Controller

The following section describes how to restore V4R1 GP7 with its original configuration from V5R3 on a WM100/1000 Controller.

NOTE

The section is written with an assumption that V4R1 GP7 was backed-up as described in "Backing up the existing V4R1 GP7 image" on page 9. If you do not have a backup image, you should contact the Extreme Networks Customer Support to get the factory default software.

The V4R1 GP7 restoration is not done from GUI, but from a low-level menu presented shortly after system boot. The restoration is done using a serial connection the Controller.

The procedure starts with reboot.

NOTE

The restore process may take between 15 and 20 minutes to finish.

To restore the V4R1 GP7 image on a WM100/1000 Controller:

1 Enter the **Rescue** mode.

To enter the Rescue mode:

a Connect to the console, using the serial port of the WM100/1000 controller.

NOTE

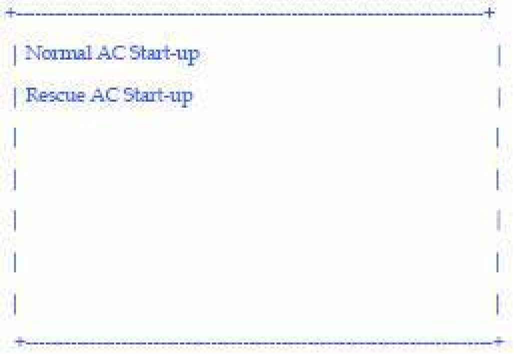
To enter the Rescue mode, you must connect to the Console serial port. You can not enter the Rescue mode using the ESA ports.

a Use the serial port of the Summit WM200/2000 Controller to connect to the console.

NOTE

To enter the ***Rescue*** *mode, you must connect to the serial port. You can not enter the* ***Rescue*** *mode by connecting to the ESA ports.*

b Reboot the Summit WM Controller. The following menu appears during the reboot process.



c Select **Rescue Ac Start-up**, and then press **Enter**. The first *repairFS* script runs after the OS initialization.

```
Attempting to Repair AC_Original Filesystems
This may take several minutes.  Please do not reboot the system
Repairing / of the original fs:
fsck 1.27 (8-Mar-2002)
/: 41649/3417568 files (0.7% non-contiguous), 284504/6825609 blocks
Repairing /home of the original fs:
fsck 1.27 (8-Mar-2002)
/home: 21/256512 files (0.0% non-contiguous), 16277/512064 blocks
Repairing /var/controller/log/cdr
fsck 1.27 (8-Mar-2002)
/var/log/extreme: 11/256512 files (0.0% non-contiguous), 16264/512071 blocks
Repairing /var/controller/log/logs
fsck 1.27 (8-Mar-2002)
/var/log/extreme1: 26/192000 files (11.5% non-contiguous), 14315/383544 blocks
Repairing /var/controller/log/reports
fsck 1.27 (8-Mar-2002)
/var/log/extreme2: 11/192000 files (0.0% non-contiguous), 14240/383544 blocks
Repairing /var/controller/log/trace
fsck 1.27 (8-Mar-2002)
/var/log/extreme3: 11/192000 files (0.0% non-contiguous), 14240/383544 blocks
repairFS: finished!
```

NOTE

The above process may take several minutes. You must not reboot the system. After the filesystem check is completed, the main rescue menu is displayed.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image Directly From The FTP Server

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 In the **Rescue** mode, press 1.

```
Your choice: 1
Backup Image List
-----------------
   1) Default image: gss-V4R0.0.50-rescue.tgz
   2) User image: gss-V4R0.0.50-rescue-user.tgz
```

3 Select the image to be restored, and then press **Enter**.

NOTE

If there is only a default image available, it will automatically get selected, bypassing the menu mentioned in Step 2.

```
Selected Restore Image is: gss-V4R0.0.50-rescue-user.tgz
This procedure is irreversible, do you wish to continue (Y/N)? Y
Performing System recovery, this may take a while...
Remove /original_root
Cleaning out normal partitions...done.
Mounting Normal Mode Partitions
mounting root...done.
mounting rest of normal mode partitions...done.
Restoring main partition...done!
Verifying volume labels...done!
Unmount all partitions to save restoration
System Recovery Complete!
Reboot the system for changes to take effect.
   << Press any key to return to previous menu. >>
```

4 In the **Main** menu, press 9. The controller reboots.

After the reboot, the system restores the backed-up image with its original configuration.

You can restore the image from the FTP server by either of the following two methods:

- First download the image from the FTP server and then restore it. For more information, see "Downloading the image from the FTP server and then restoring it" on page 66.
- Restore the image directly from the FTP server without downloading it. For more information, "Restoring the image directly from the FTP server without downloading it" on page 67.

Downloading the image from the FTP server and then restoring it

To download the image from the FTP server carry out the following procedure:

1 Configure the FTP settings.

To configure the FTP settings:

a From the Main menu, select 4. The following menu is displayed.

```
   1) Enter FTP Settings
   2) Change ftp server ip address
   3) Change ftp port
   4) Change user name
   5) Change password
   6) Change ftp directory
   7) Change file name
   8) Display current ftp settings
   9) Display backup images
   10) Download image from ftp server
   11) Upload image onto the ftp server
   12) Return to the main menu
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
```

b Enter the FTP information.

```
ftp://administrator:abc123@192.168.4.181//tester/v5r1/backup-user-rescue.tgz
```

NOTE

When you are backing-up the image, you must follow the naming convention given below: filename-user-rescue.tgz. If you haven't followed this naming convention while saving your backup file, the backup file will not download to the controller from the FTP server. In such a case, you must restore the image directly from the FTP server. For more information see, "Restoring the image directly from the FTP server without downloading it" on page 67.

c In the FTP menu, press 10. The following screen is displayed.

```
Your choice: 10
File is user image
Warning! In order to continue previous user image will be removed (if it exists)
Proceed (Y/N): Y
Attempting to download an image from the ftp server. Please be patient
Please verify that image has successfully been downloaded (Option 9 from FTP
Menu)
   << Press any key to return to previous menu. >>
```

NOTE

Download times are usually much faster than upload times.

2 Follow Steps 1 to 4 of "Restoring V4R1 GP7 image from V5R3 on the Summit WM100/1000 Controller" on page 63

Restoring the image directly from the FTP server without downloading it

To restore the image directly from the FTP server without downloading it:

1 Return to the main menu.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image Directly From The FTP Server

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

2 Enter **5**. The following menu is displayed.

```
   1) Display Current Rescue Interface Info
   2) Enter Interface Information
   3) Change ip address
   4) Change ip mask
   5) Change default gateway
   6) Test interface by ICMP (ping)
   7) Return to the main menu Connect to the console, using the serial port of
      the Controller.
```

a In the **Rescue** mode, press **2**. The following message is displayed.

```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
```

b Enter the following information:

- IP address of your controller's Management Ethernet Port
- IP mask
- IP address of Gateway

The system configures the interface and returns to the main menu.

```
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
```

3 Press any key to return to the main menu

4 Enter **4** in the Main menu to configure the FTP settings. The following menu is displayed.

```
FTP Menu
   1) Enter FTP Settings
   2) Change ftp server ip address
   3) Change ftp port
   4) Change user name
   5) Change password
   6) Change ftp directory
   7) Change file name
   8) Display current ftp settings
   9) Display backup images
   10) Download image from ftp server
   11) Upload image onto the ftp server
   12) Return to the main menu
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
```

5 Enter the FTP information.

```
ftp://administrator:abc123@192.168.4.181//tester/v5r1/backup.tgz
```

6 Return to the main menu

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image Directly From The FTP Server

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

7 Enter **7**.

```
Your choice: 7
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.191 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: /tester/v5r1/, file backup.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

8 Enter **Y**.

After the reboot, the system restores the backed-up image with its original configuration

Restoring V4R2 image from V5R3 on the Summit WM20 Controller

The following section describes how to restore V4R2 GP1 with its original configuration from V5R3 on the Summit WM20 Controller.

NOTE

The section is written with an assumption that V4R2 was backed-up as described in "Backing up the existing V4R2 image on the Summit WM20 Controller" on page 18. If you do not have a backup image, you should contact the Extreme Networks Customer Support to get the factory default software.

The V4R2 restoration is not done from GUI, but from a low-level menu presented shortly after system boot.

The procedure starts with reboot.

NOTE

The restore process may take between 15 and 20 minutes to finish.

To restore the V4R2 image on the Summit WM20 Controller:

1 Use the serial port of the Summit WM20 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port. You can not enter the **Rescue** mode by connecting to the ESA ports.*

2 Reboot the Summit WM Controller. The following menu appears during the reboot process.

```
----------------------------------------------------------------
 0: Main Mode
 1: Rescue Mode
----------------------------------------------------------------
```

3 Press 1 to enter the **Rescue** mode. The following menu is displayed.

```
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image Directly From The FTP Server
   7) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

4 Enter **5**. The following menu is displayed.

```
   1) Display Current Rescue Interface Info
   2) Enter Interface Information
   3) Change ip address
   4) Change ip mask
   5) Change default gateway
   6) Test interface by ICMP (ping)
   7) Return to the main menu
```

5 Configure the Network Interface.

To configure the Network Interface:

a In the **Network Interface** menu, press **2**, and then enter the following:

- IP address of your WM200/2000 Controller's Management Ethernet Port
- IP mask
- IP address of Gateway

```
Your choice> 2
Please enter Interface information
Format <ip>:<netmask> <gw optional>
Input: 192.168.1.201:255.255.255.0 192.168.1.1
Configuring interface ...
Setting up network interface ...Done!
```

6 Press any key to return to the **Main** menu.

7 Enter **4** in the Main menu to configure the FTP settings. The **FTP** menu is displayed.

```
   1) Enter FTP Settings
   2) Change ftp server ip address
   3) Change ftp port
   4) Change user name
   5) Change password
   6) Change ftp directory
   7) Change file name
   8) Display current ftp settings
   9) Display backup images
   10) Download image from ftp server
   11) Upload image onto the ftp server
   12) Return to the main menu
Your choice: 1
Command syntax: ftp://<user>:<password>@<ftp_ip>:<port>/<directory&file>
~port information is optional: the default value is 21~
Please enter ftp info:
```

8 Enter the FTP information.

```
ftp://administrator:abc123@192.168.4.181//tester/v5r1/backup.tgz
```

9 Return to the **Main** menu by pressing any key.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image Directly From The FTP Server
   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

10 Enter **7**. The following message is displayed.

```
Your choice: 7
Make sure correct information is entered for Interface and FTP settings.
IP: 192.168.4.191 netmask 255.255.255.0 gateway:
FTP Settings: IP 192.168.4.181, port 21, user: administrator, password: abc123,
directory: /tester/v5r1/, file backup.tgz
This procedure is irreversible, do you wish to continue (Y/N)?
```

11 Enter **Y**

After the reboot, the system restores the backed-up image with its original configuration.

Restoring V5R1 image from V5R3 on the Summit WM20 Controller

The procedure for restoring V5R1 on the Summit WM100/1000 Controller is same as described in "Restoring V4R2 image from V5R3 on the Summit WM20 Controller" on page 69.

5 Using the Console Port

This chapter describes how to use the console ports in the following models of the Summit WM Controllers:

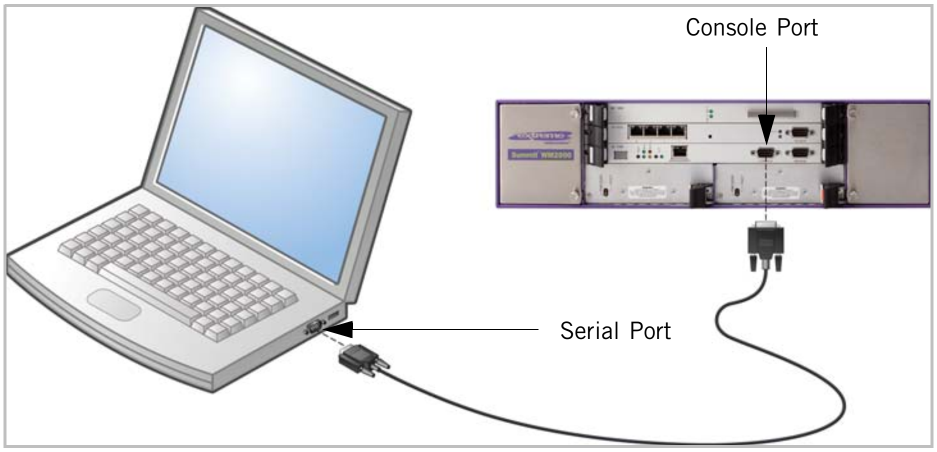
- Summit WM200/2000 Controller
- Summit WM20 Controller
- Summit WM100/1000 Controller

Using the Console Port in the Summit WM200/2000 Controller

In order to get into the **Rescue** mode in the Summit WM200/2000 Controller, you must connect your laptop to controller's **Console Port** via the Null Modem DB9 F- F (Female to Female) Cable.

The following illustration shows the cable connection between a laptop and the Summit WM200/2000 Controller.

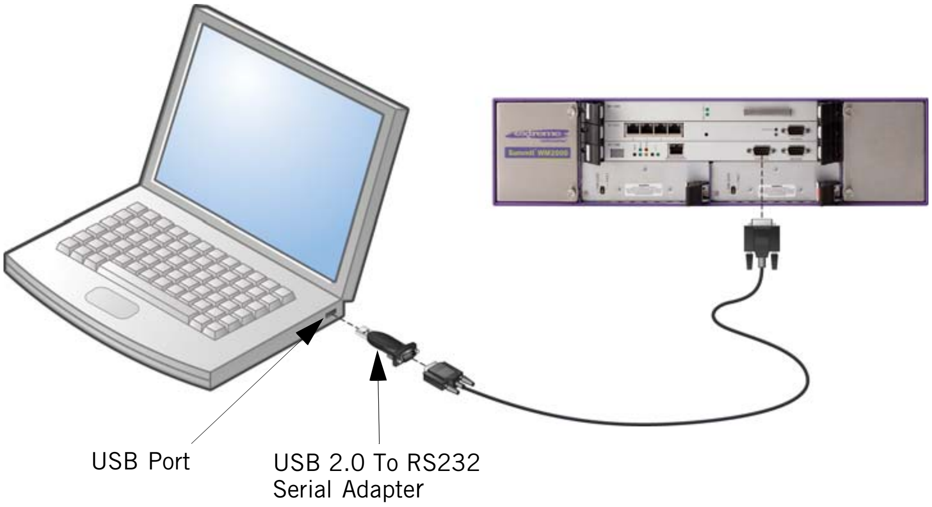
Figure 4: Connection between the Summit WM200/2000 Controller and laptop with serial port.



If your laptop has a USB port instead of a serial port, you must use the USB 2.0 To RS232 Serial Adapter to connect the Null Model DB9 F-F Cable to the laptop.

The following illustration shows the cable connection between the laptop with a USB port and the Summit WM200/2000 Controller.

Figure 5: Connection between the Summit WM Controller and laptop with USB Port



Using a terminal program of choice (for example, Hyperterm) establish a connection between the Summit WM200/2000 Controller and the laptop, using the corresponding COM port. You must configure the following connection settings: For more information on how to configure the connection settings, see Step 7 of "Using the Console Port in the Summit WM20 Controller" on page 74.

- **Speed** – 9600
- **Databits** – 8
- **Parity** – None
- **Stop Bits** – 1
- **Flow Control** – None

NOTE

If you need to remove the DB9 (F-F cable) in the midst of your session, you must first run the ***exit*** *command to return to the login screen, and then remove the cable.*

Using the Console Port in the Summit WM20 Controller

Before you start hooking up the cable to access the **Rescue** mode, you must install the virtual driver from Silicon Laboratories on your laptop.

To connect to the console port:

1. Install the virtual serial driver by Silicon Laboratories Inc. on the laptop. You only need to install the serial driver once. You do not need to repeat installing the software each time you connect to the port.
2. The CP210x USB to UART Bridge VCP drivers are provided by Silicon Laboratories Inc. Depending on the OS of your computer, click on the appropriate "VCP Driver Kit" link on the web page given below. Note that this URL is subject to change.

   https://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx

3 With a normal USB (male A/B) cable, connect the B end to the Summit WM20 Controller and the A end to the laptop. The driver recognizes the connection and installs a serial device (Com #).

To determine the actual number assigned to the device, navigate to **Control Panel** > **System** > **Hardware** > **Device Manager** > **Ports (COM & LPT)**.

4 Using a terminal program of choice (for example, Hyperterm) establish a connection to the Summit WM20 Controller using the corresponding COM device.

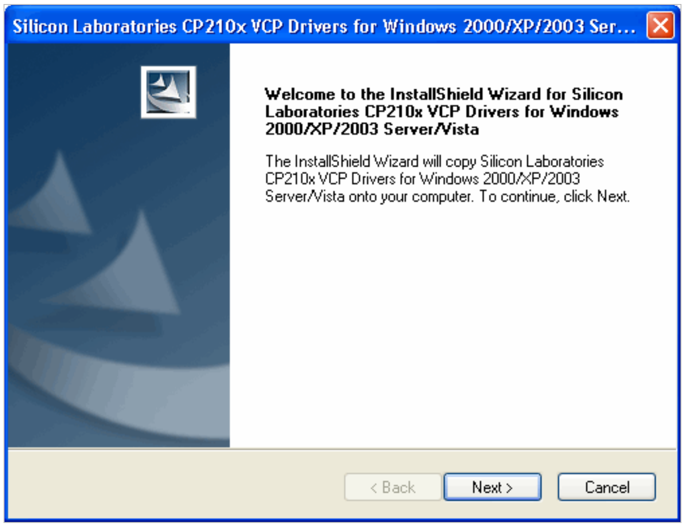
The connection settings are 9600 8N1 no flow (9600 bps, 8 bits, no parity, 1 stop bit, no flow).

To install the driver:

NOTE

The following procedure is applicable for installing CP210x VCP driver specific to Windows 2000/XP/2003 Server/Vista.

a Double-click on the *.exe* file. The **setup wizard** is launched.



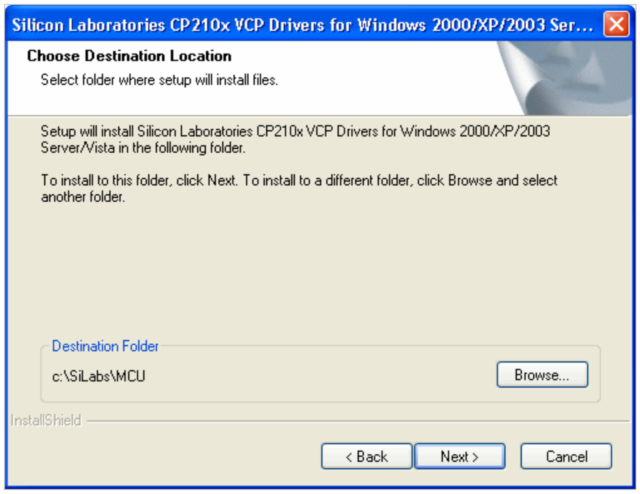
Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Ser...

Welcome to the InstallShield Wizard for Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/Vista

The InstallShield Wizard will copy Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/Vista onto your computer. To continue, click Next.

b Click **Next**. The **License Agreement** window opens.

c Select the **I accept the terms of the license agreement** radio button, and then click **Next**. The **Destination Location** window opens.


Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Ser...

Choose Destination Location

Select folder where setup will install files.

Setup will install Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/Vista in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

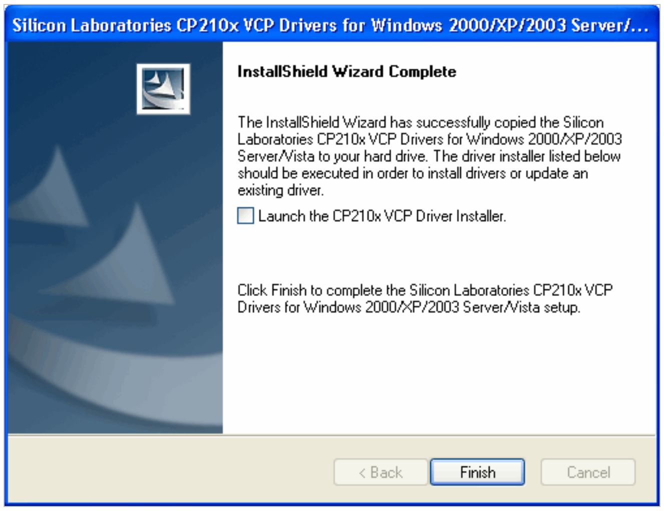
Destination Folder

c:\SiLabs\MCU

If you want to change the default destination (C:\Silabs\MU), you can do so by clicking on the **Browse** button and navigating to the destination, where you want to save the driver.

d Click **Next**. The **Ready to Install the program** window opens.

e Click **Install**. The wizard copies the driver to your hard drive, and the **Finish** window opens.


Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/...

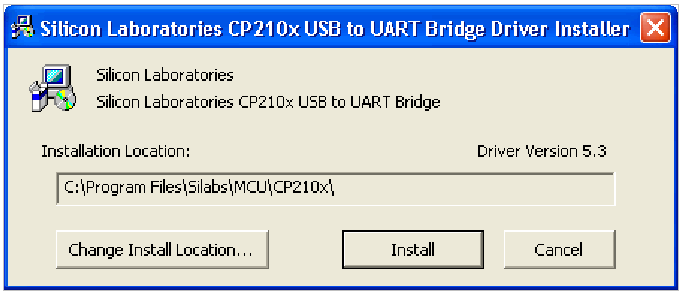
InstallShield Wizard Complete

The InstallShield Wizard has successfully copied the Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/Vista to your hard drive. The driver installer listed below should be executed in order to install drivers or update an existing driver.

□ Launch the CP210x VCP Driver Installer.

Click Finish to complete the Silicon Laboratories CP210x VCP Drivers for Windows 2000/XP/2003 Server/Vista setup.

f Select **Launch the CP210x VCP Driver Installer** checkbox, and then click **Finish**. The **Driver Installer** opens.


Silicon Laboratories CP210x USB to UART Bridge Driver Installer

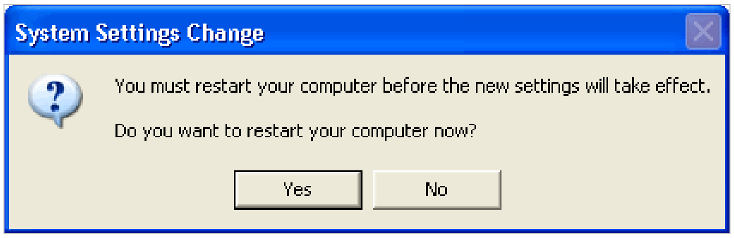
Silicon Laboratories

Silicon Laboratories CP210x USB to UART Bridge

Installation Location: Driver Version 5.3

C:\Program Files\Silabs\MCU\CP210x\

g Click **Install**. The **System Settings Change** window opens.



System Settings Change

You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

h Click **Yes**. The system reboots and the driver is installed.

5 Connect your laptop to the Summit WM20 Controller via USB A/B Device Cable as shown in Figure 6.

6 Determine the actual **Communications Port #** assigned to the device.

To determine the actual Communications Port # assigned to the device:

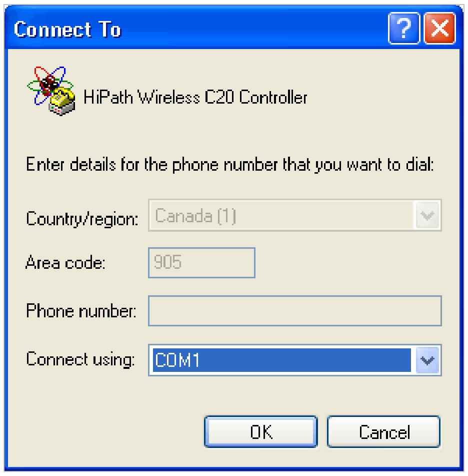
a On the **Start** menu, point to **Control Panel**, point to **System**, point to **Hardware**, point to **Device Manager**, and then click **Ports** (**Comm &LPT**).

b Check the **Communications Port** number assigned to the device.

7 Establish the connection between your laptop and the Summit WM20 Controller.

To establish the connection:

a Point to **All Programs**, point to **Accessories**, point to **Communication**, and then click terminal program of your choice (for example, **Hyperterminal**). The **Connect to** window opens.



Connect To

HiPath Wireless C20 Controller

Enter details for the phone number that you want to dial:

Country/region: Canada (1)

Area code: 905

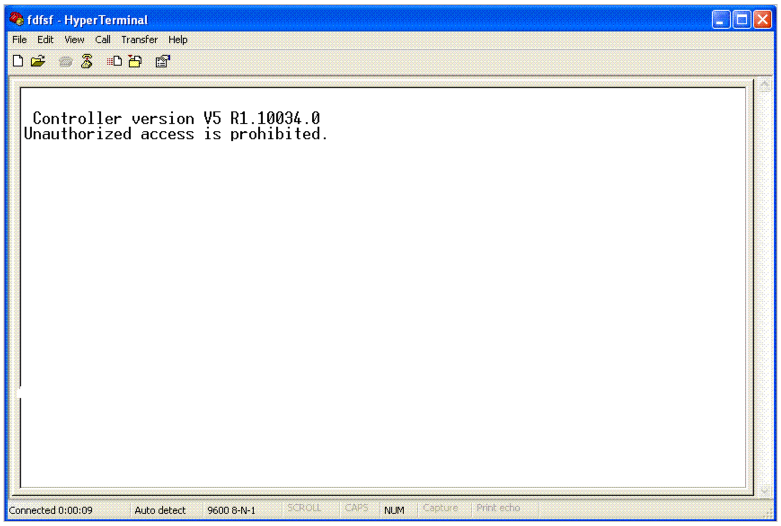
Phone number:

Connect using: COM1

b From the **Connect using** drop-down menu, select the communications port # assigned to the device, and then click **OK**. The **Port Settings** window opens.

c In the **Port Settings** window, configure the following settings, and then click **OK**. The connection is established.

- **Speed** – 9600
- **Databits** – 8
- **Parity** – None
- **Stop Bits** – 1
- **Flow Control** – None

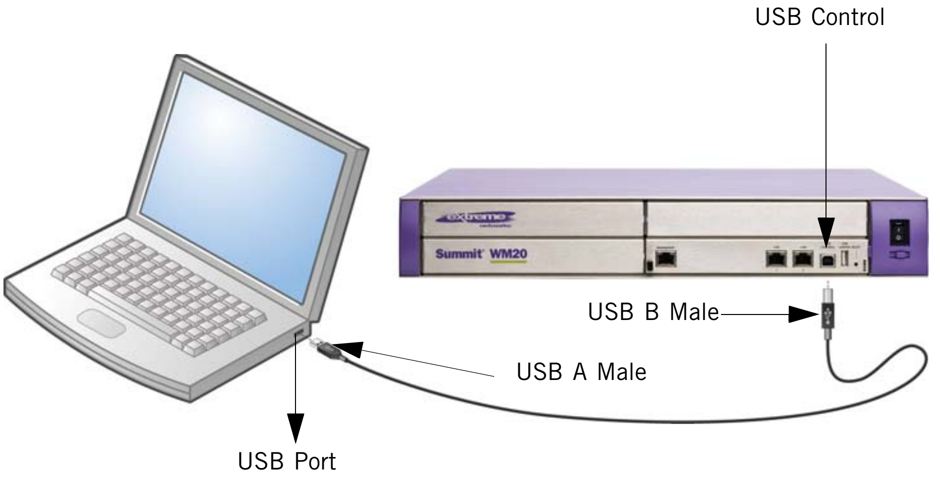


```
 Controller version V5 R1.10034.0
Unauthorized access is prohibited.
```

The Summit WM20 Controller is ready to be booted into the **Rescue** mode.

The following illustration shows the cable connection between a laptop and the Summit WM20 Controller.

Figure 6: Connection between the Summit WM20 Controller and laptop



Using the Console Port in the Summit WM100/1000 Controller

The cable connection between the Summit WM1000 Controller and laptop to access the **Rescue** mode is same as described in "Using the Console Port in the Summit WM200/2000 Controller" on page 73.

6 Performing system maintenance

You can perform various system maintenance tasks, including:

- Changing the log level
- Setting a poll interval for checking the status of the Altitude APs (Health Checking)
- Enabling and defining parameters for Syslog event reporting
- Forcing an immediate system shutdown, with or without reboot
- Resetting an Altitude AP to its factory defaults

Syslog event reporting uses the syslog protocol to relay event messages to a centralized event server on your enterprise network. In the protocol a device generates messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.

NOTE

The log statements ***Low water mark level was reached*** *and* ***Incoming message dropped, because of the rate limiting mechanism*** *indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way. For more information, see Chapter 7, "Logs, traces, audits, and DHCP messages."*

NOTE

The term, 'Altitude AP', is used in this document to encompass all three variants - Altitude AP, Outdoor AP (Siemens), and Altitude 802.11n AP. The variants are only specifically identified in the documentation where it is necessary to do so.

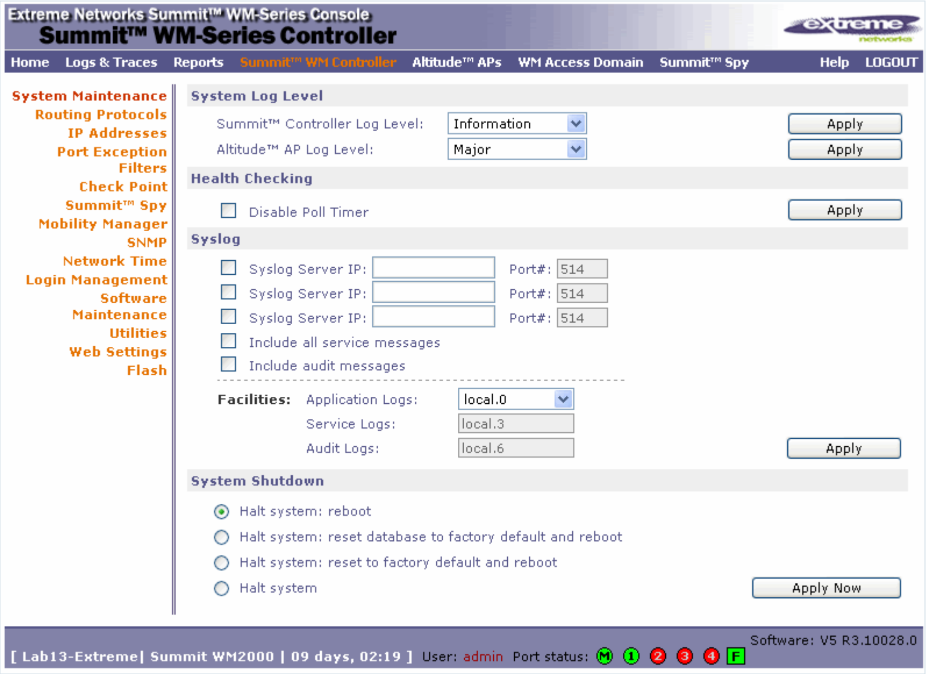
The topics in this chapter are organized as follows:

- Changing logs levels and enabling Syslog event reporting
- Enabling/disabling poll timer
- Forcing immediate system shut down
- Resetting the Wireless APs to their factory default settings

Changing logs levels and enabling Syslog event reporting

To change the log levels:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.



System Log Level

Summit™ Controller Log Level: Information

Altitude™ AP Log Level: Major

Health Checking

□ Disable Poll Timer

Syslog

□ Syslog Server IP: Port#: 514

□ Syslog Server IP: Port#: 514

□ Syslog Server IP: Port#: 514

□ Include all service messages

□ Include audit messages

Facilities: Application Logs: local.0

Service Logs: local.3

Audit Logs: local.6

System Shutdown

● Halt system: reboot

○ Halt system: reset database to factory default and reboot

○ Halt system: reset to factory default and reboot

○ Halt system

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 02:19] User: admin Port status: M 1 2 3 4 F

2 In the **System Log Level** section, from the **Summit Controller Log Level** drop-down list, select the least severe log level for the Controller that you want to receive: **Information**, **Minor**, **Major**, **Critical**. For example, if you select **Minor**, you receive all **Minor**, **Major** and **Critical** messages. If you select **Major** you receive all **Major** and **Critical** messages. The default is **Information**.

3 Click **Apply**.

4 From the **Altitude AP Log Level** drop-down list, select the least severe log level for the AP that you want to receive: **Information**, **Minor**, **Major**, **Critical**. The default is **Critical**.

5 Click **Apply**.

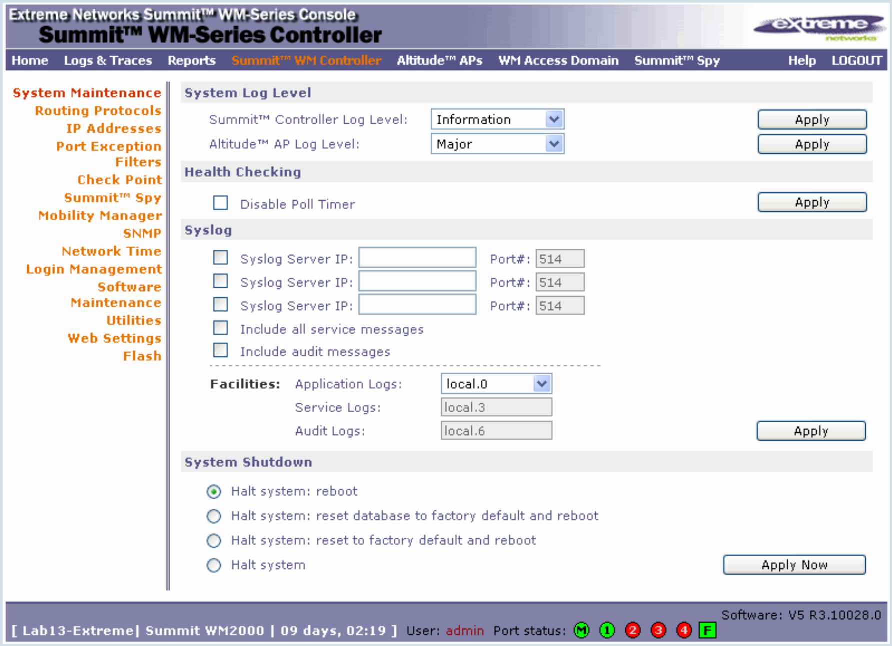
Enabling/disabling poll timer

To enable/disable poll timer:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 To disable the poll timer, select the **Disable Poll Timer** checkbox in the **Health Checking** section.

3 To enable the poll timer, uncheck the **Disable Poll Timer** checkbox in the **Health Checking** section.



System Log Level

Summit™ Controller Log Level: Information

Altitude™ AP Log Level: Major

Health Checking

☐ Disable Poll Timer

Syslog

☐ Syslog Server IP: Port#: 514

☐ Syslog Server IP: Port#: 514

☐ Syslog Server IP: Port#: 514

☐ Include all service messages

☐ Include audit messages

Facilities: Application Logs: local.0

Service Logs: local.3

Audit Logs: local.6

System Shutdown

● Halt system: reboot

○ Halt system: reset database to factory default and reboot

○ Halt system: reset to factory default and reboot

○ Halt system

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 02:19] User: admin Port status: M 1 2 3 4 F

4 Click **Apply**.

To enable and define parameters for Syslog:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 In the **Syslog** section, to enable the **Syslog** function for up to three syslog servers, select the appropriate checkboxes.

3 For each enabled syslog server, in the **IP** box, type a valid IP address for the server on the network.

4 For each enabled syslog server, in the **Port #** box, type a valid port number to connect on. The default port for syslog is **514**.

5 To include all system messages, select the **Include all service messages** checkbox. If the box is not selected, only component messages (logs and traces) are relayed. This setting applies to all three servers. The additional service messages are:

- DHCP messages reporting users receiving IP addresses
- Startup Manager Task messages reporting component startup and failure

6 To include audit messages, select the **Include audit messages** checkbox.

7 From the **Application Logs** drop-down list, select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

8 If the **Include all service messages** checkbox is selected, the **Service Logs** drop-down list becomes selectable. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

9 If you selected the **Include audit messages** checkbox, the **Audit Logs** drop-down list becomes available. Select the log level (local.0 - local.6) to be sent to the syslog server. This setting applies all three servers.

10 To apply your changes, click **Apply**.

NOTE

The syslog daemon must be running on both the Summit WM Controller and on the remote syslog server before the logs can be synchronized. If you change the log level on the Summit WM Controller, you must also modify the appropriate setting in the syslog configuration on remote syslog server.

Table 4 displays Syslog and Controller, Access Points and Software event log mapping.

Table 4: Syslog and Controller, Access Points and Software event log mapping

Syslog Event	Controller, Access Points and Software Event
LOG_CRIT	Critical
LOG_ERR	Major
LOG_WARNING	Minor
LOG_INFO	Information
LOG_DEBUG	Trace

Forcing immediate system shut down

To force immediate system shutdown:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 To shut down the system, including associated Altitude APs, select the appropriate shut down option:

- Halt system: reboot
- Halt system: reset database to factory default and reboot – Restores all aspects of the system configuration to the initial settings. However, the Management IP address and license key are preserved. This permits the user to remain connected through the Management interface.
- Halt system: reset to factory default and reboot – Resets the entire system configuration to the factory shipping state. The Management IP address reverts to 192.168.10.1 and the license key is removed.
- Halt system – The system enters the halted state, which stops all functional services and the application. To restart the system, the power to the system must be reset.

3 Click **Apply Now**. The system is immediately halted.

Resetting the Wireless APs to their factory default settings

You can reset the Altitude AP and the Outdoor AP to their factory default settings.

NOTE

The term, 'Altitude AP', is used in this document to encompass all three variants - Altitude AP, Outdoor AP (Siemens), and Altitude 802.11n AP. The variants are only specifically identified in the documentation where it is necessary to do so.

Resetting an Altitude AP to its factory default settings

The AP boot-up sequence includes a random delay interval, followed by a vulnerable time interval. The LEDs flash in a particular sequence to indicate that the AP is in the vulnerable time interval (2 seconds). For more information, see the *Summit WM User Guide*.

If you power up the AP and interrupt the power during the vulnerable time interval three consecutive times, the next time the AP reboots, it will restore its factory defaults including the user password and the default IP settings.

CAUTION

The restoration of factory default settings does not erase the non-volatile log.

To reset the Altitude 350-2 AP to its factory default settings:

1. Switch off, and then switch on the Altitude AP. The Altitude AP reboots.
2. Switch off, and then switch on the Altitude AP during the vulnerable time interval.

   NOTE

   You should refer to the Altitude AP's LED pattern to determine the vulnerable period. For more information, see Summit WM User Guide.

3. Repeat Step 2 two more times.

   When the Altitude AP reboots for the fourth time, after having its power supply interrupted three consecutive times, it restores its factory default settings. The Altitude AP then reboots again to put the default settings into effect.

   NOTE

   You should refer to the Altitude AP's LED pattern to confirm that the Altitude AP is set to its factory defaults. For more information, see Summit WM User Guide.

Reset button (Hardware)

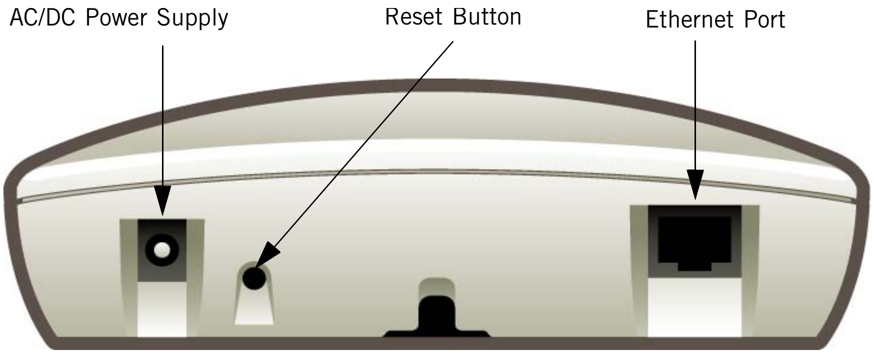
Some models of the Altitude AP have a reset button. If your model is equipped with a reset button, you can set it to its factory default settings by pressing and holding the reset button for approximately six seconds.

NOTE

If you press the reset button and do not hold it over six seconds, the Altitude AP will merely reboot, and not reset to its factory defaults.

The following figure illustrates the location of the reset button on the Altitude 350-2 APs.

Figure 7: Position of the reset button in the Altitude 350-2 AP



Resetting the Outdoor AP to its factory default settings

All models of the Outdoor AP have a reset button.

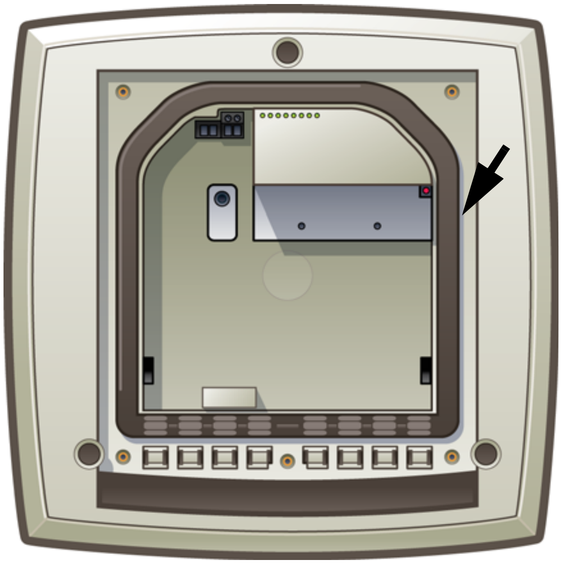
You can set the Outdoor AP to its factory default settings by pressing and holding the reset button for approximately six seconds.

NOTE

If you press the reset button and do not hold it over six seconds, the Outdoor AP will merely reboot, and not reset to its factory defaults.

The following figure illustrates the location of the reset button on the Outdoor AP.

Figure 8: Position of the reset button with the housing cover removed



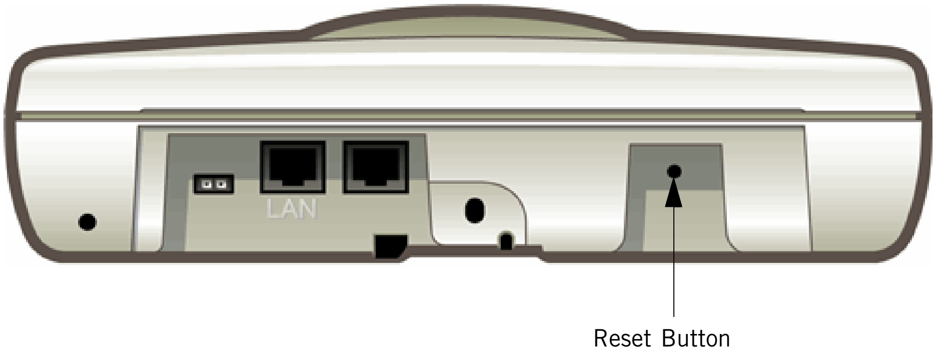
NOTE

The reset button is located below the housing cover beside the sockets for the external antennas. To access the reset button, you must remove the housing cover. For more information, see the Outdoor AP Installation Guide.

Resetting the Altitude 450/451 (802.11n) AP to its factory default settings

You can set the Altitude 802.11n AP to its factory default settings by pressing and holding the reset button for approximately four seconds.

Figure 9: Position of the reset button in the Altitude 802.11n AP



NOTE

If you press the reset button and do not hold it over four seconds, the Altitude 802.11n AP will merely reboot, and not reset to its factory defaults.

7 Logs, traces, audits, and DHCP messages

The Summit WM Controller generates four types of messages:

- **Logs (including alarms)** – Messages that are triggered by events
- **Traces** – Messages that display activity by component, for system debugging, troubleshooting and internal monitoring of software

CAUTION

*In order for the **Debug Info** option on the **Altitude AP Traces** page to return trace messages, this option must be enabled while Altitude AP debug commands are running. To do so, you need to run a Altitude AP CLI command to turn on a specific Altitude AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see the Summit WM CLI Reference Guide.*

Because Altitude AP debugging can affect the normal operation of Altitude AP service, enabling debugging is not recommended unless specific instructions are provided.

- **Audits** – Messages that record administrative changes made to the system
- **DHCP** – Messages that record DHCP service events

The topics in this chapter are organized as follows:

- Working with logs
- Working with trace messages
- Viewing audit messages
- Viewing DHCP messages
- Viewing software upgrade and operating system patch messages
- Viewing restore/import messages

Working with logs

The log messages contain the time of event, severity, source component, and any details generated by the source component. Log messages are divided into three groups:

- Summit WM Controller logs
- Altitude AP logs
- Login logs

Log severity levels

Log messages are classified at four levels of severity:

- Information (the activity of normal operation)
- Minor (alarm)
- Major (alarm)

- Critical (alarm)

The alarm messages (minor, major or critical log messages) are triggered by activities that meet certain conditions that should be known and dealt with. The following are examples of events on the Summit WM Controller that generate an alarm message:

- Reboot due to failure
- Software upgrade failure on the Summit WM Controller
- Software upgrade failure on the Altitude AP
- Detection of rogue access point activity without valid ID
- Availability configuration not identical on the primary and secondary Summit WM Controller

If SNMP is enabled on the Summit WM Controller, alarm conditions will trigger a trap in SNMP (Simple Network Management Protocol). An SNMP trap is an event notification sent by the managed agent (a network device) to the management system to identify the occurrence of conditions.

NOTE

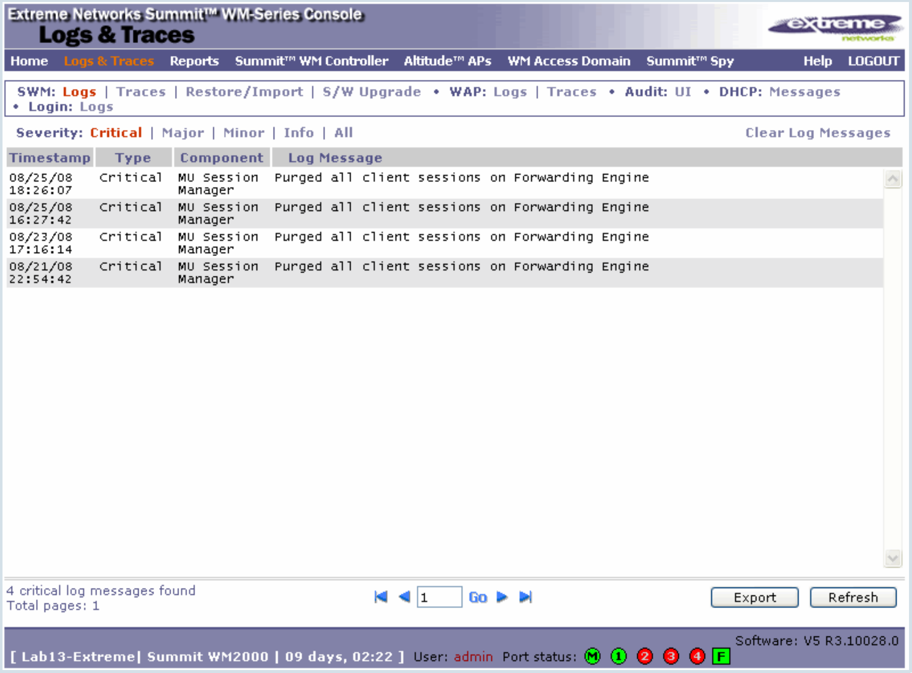
The log statements ***Low water mark level was reached*** *and* ***Incoming message dropped, because of the rate limiting mechanism*** *indicate that there is a burst of log messages coming to the event server and the processing speed is slower than the incoming rate of log messages. These messages do not indicate that the system is impaired in any way.*

Viewing Summit WM Controller logs

To view Summit WM Controller logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **SWM: Logs** tab. The Summit WM Controller log page is displayed and the events are displayed in chronological order:



Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
Severity: Critical | Major | Minor | Info | All
Clear Log Messages
Go
Export
Refresh

Timestamp	Type	Component	Log Message
08/25/08 18:26:07	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/25/08 16:27:42	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/23/08 17:16:14	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/21/08 22:54:42	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine

4 critical log messages found
Total pages: 1

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:22] User: admin Port status: M 1 2 3 4 F

3 To sort the events by **Timestamp**, **Type**, or **Component**, click the appropriate column heading.

4 To filter the events by severity, **Critical**, **Major**, **Minor**, **Info**, and **All**, click the appropriate log severity.

5 To refresh the Summit WM Controller log page, click **Refresh**.

6 To export the Summit WM Controller log page, click **Export**. The **File Download** dialog is displayed.

7 Do one of the following:

- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file.
- Click **Save**.

NOTE

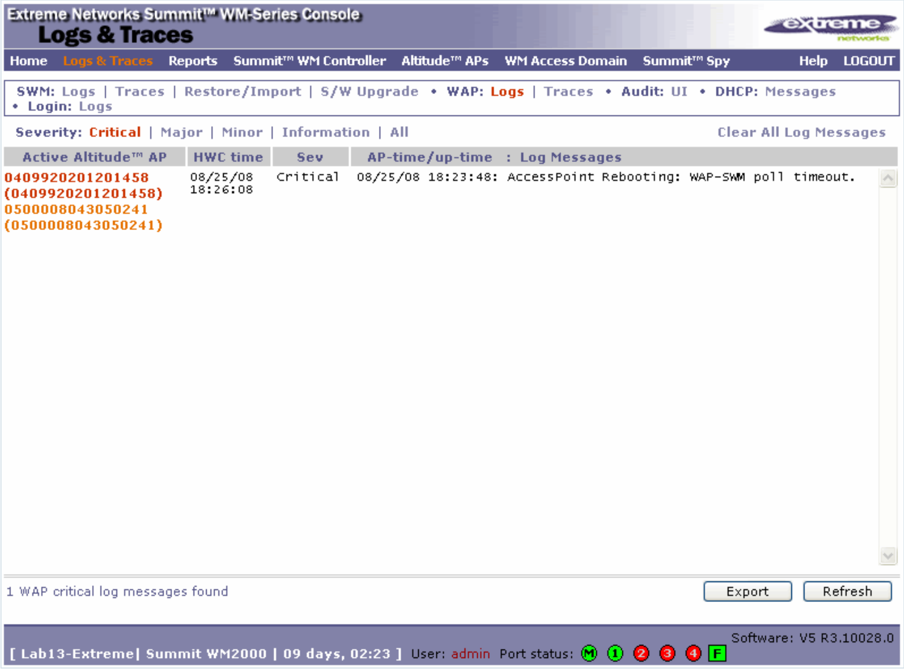
The component "Langley" is the term for the inter-process messaging infrastructure on the Summit WM Controller.

Viewing Altitude AP logs

To view Altitude AP logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **WAP: Logs** tab. The Altitude AP log page is displayed and the events are displayed in chronological order:


Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
Severity: Critical | Major | Minor | Information | All
Clear All Log Messages
Export
Refresh

Active Altitude™ AP	HWC time	Sev	AP-time/up-time : Log Messages
0409920201201458 (0409920201201458) 0500008043050241 (0500008043050241)	08/25/08 18:26:08	Critical	08/25/08 18:23:48: AccessPoint Rebooting: WAP-SWM poll timeout.

1 WAP critical log messages found

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:23] User: admin Port status: M 1 2 3 4 F

3 In the **Active Altitude AP** list, click a Altitude AP to view the log events for that particular Altitude AP.

4 To sort the events by **Timestamp** or **Severity**, click the appropriate column heading.

5 To filter the events by severity, **Critical**, **Major**, **Minor**, **Information**, and **All**, click the appropriate log severity.

6 To refresh the Summit WM Controller log page, click **Refresh**.

7 To export the Summit WM Controller log page, click **Export**. The **File Download** dialog is displayed.

8 Do one of the following:

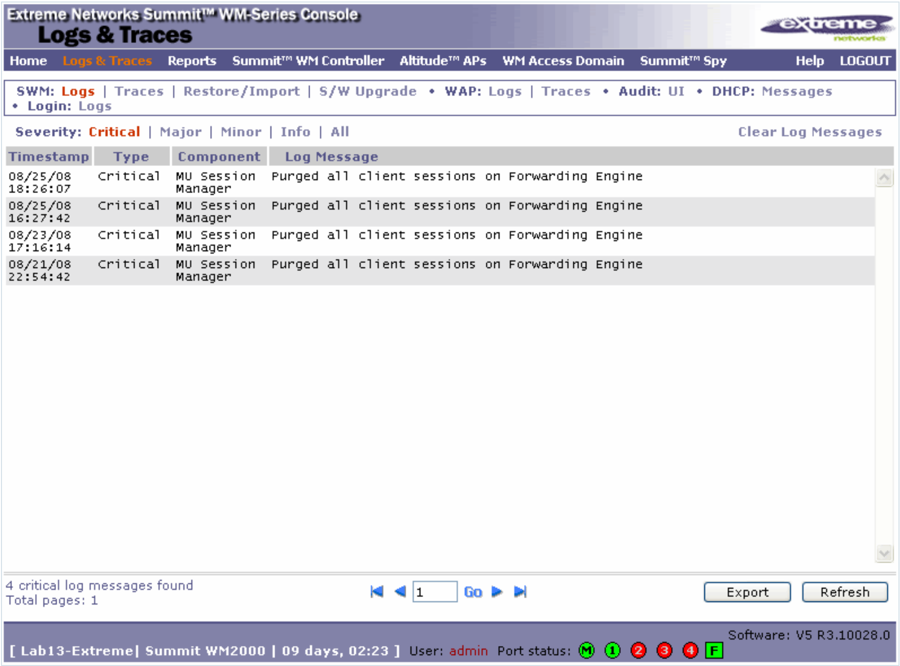
- To open the log file, click **Open**.
- To save the log file, click **Save**, and then navigate to the directory location you want to save the file.
- Click **Save**.

Clearing Summit WM Controller logs

To clear Summit WM Controller logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **SWM: Logs** tab. The Summit WM Controller log page is displayed and the events are displayed in chronological order:


Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages
• Login: Logs
Severity: Critical | Major | Minor | Info | All
Clear Log Messages
1
Go
Export
Refresh

Timestamp	Type	Component	Log Message
08/25/08 18:26:07	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/25/08 16:27:42	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/23/08 17:16:14	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine
08/21/08 22:54:42	Critical	MU Session Manager	Purged all client sessions on Forwarding Engine

4 critical log messages found
Total pages: 1

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:23] User: admin Port status: M 1 2 3 4 F

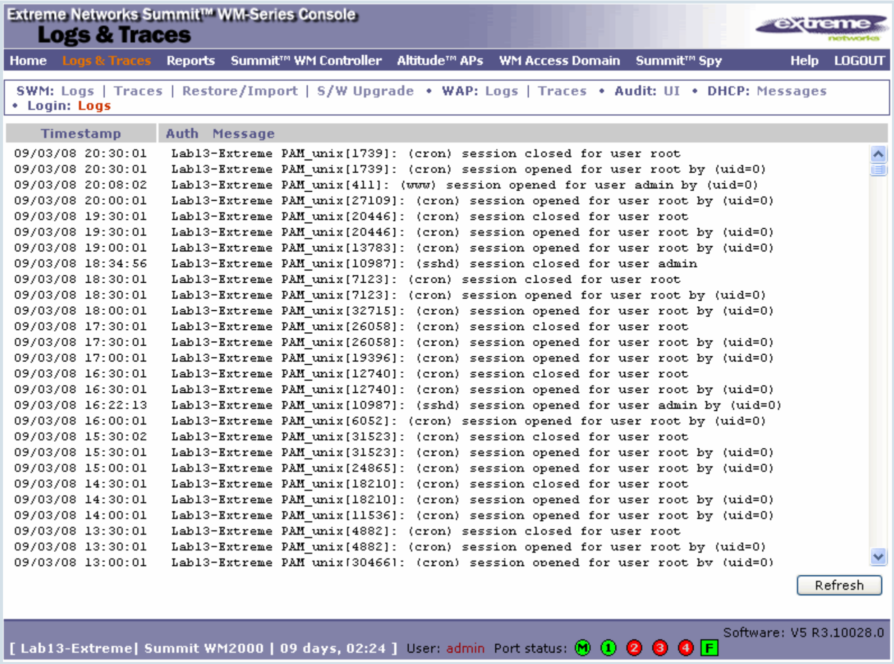
3 To clear the logs, click **Clear Log Messages**.

4 To confirm the deletion of the Summit WM Controller log messages, click **Ok**. The Summit WM Controller log messages are deleted.

To view login logs:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **Login: Logs** tab. The Login: Logs page is displayed and the login events are displayed in chronological order:


Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
Refresh
[Lab13-Extreme| Summit WM2000 | 09 days, 02:24] User: admin Port status: M 1 2 3 4 F
Software: V5 R3.10028.0

```
Timestamp          Auth   Message
09/03/08 20:30:01   Lab13-Extreme PAM_unix[1739]: (cron) session closed for user root
09/03/08 20:30:01   Lab13-Extreme PAM_unix[1739]: (cron) session opened for user root by (uid=0)
09/03/08 20:08:02   Lab13-Extreme PAM_unix[411]: (www) session opened for user admin by (uid=0)
09/03/08 20:00:01   Lab13-Extreme PAM_unix[27109]: (cron) session opened for user root by (uid=0)
09/03/08 19:30:01   Lab13-Extreme PAM_unix[20446]: (cron) session closed for user root
09/03/08 19:30:01   Lab13-Extreme PAM_unix[20446]: (cron) session opened for user root by (uid=0)
09/03/08 19:00:01   Lab13-Extreme PAM_unix[13783]: (cron) session opened for user root by (uid=0)
09/03/08 18:34:56   Lab13-Extreme PAM_unix[10987]: (sshd) session closed for user admin
09/03/08 18:30:01   Lab13-Extreme PAM_unix[7123]: (cron) session closed for user root
09/03/08 18:30:01   Lab13-Extreme PAM_unix[7123]: (cron) session opened for user root by (uid=0)
09/03/08 18:00:01   Lab13-Extreme PAM_unix[32715]: (cron) session opened for user root by (uid=0)
09/03/08 17:30:01   Lab13-Extreme PAM_unix[26058]: (cron) session closed for user root
09/03/08 17:30:01   Lab13-Extreme PAM_unix[26058]: (cron) session opened for user root by (uid=0)
09/03/08 17:00:01   Lab13-Extreme PAM_unix[19396]: (cron) session opened for user root by (uid=0)
09/03/08 16:30:01   Lab13-Extreme PAM_unix[12740]: (cron) session closed for user root
09/03/08 16:30:01   Lab13-Extreme PAM_unix[12740]: (cron) session opened for user root by (uid=0)
09/03/08 16:22:13   Lab13-Extreme PAM_unix[10987]: (sshd) session opened for user admin by (uid=0)
09/03/08 16:00:01   Lab13-Extreme PAM_unix[6052]: (cron) session opened for user root by (uid=0)
09/03/08 15:30:02   Lab13-Extreme PAM_unix[31523]: (cron) session closed for user root
09/03/08 15:30:01   Lab13-Extreme PAM_unix[31523]: (cron) session opened for user root by (uid=0)
09/03/08 15:00:01   Lab13-Extreme PAM_unix[24865]: (cron) session opened for user root by (uid=0)
09/03/08 14:30:01   Lab13-Extreme PAM_unix[18210]: (cron) session closed for user root
09/03/08 14:30:01   Lab13-Extreme PAM_unix[18210]: (cron) session opened for user root by (uid=0)
09/03/08 14:00:01   Lab13-Extreme PAM_unix[11536]: (cron) session opened for user root by (uid=0)
09/03/08 13:30:01   Lab13-Extreme PAM_unix[4882]: (cron) session closed for user root
09/03/08 13:30:01   Lab13-Extreme PAM_unix[4882]: (cron) session opened for user root by (uid=0)
09/03/08 13:00:01   Lab13-Extreme PAM_unix[30466]: (cron) session opened for user root by (uid=0)
```

To refresh the **Login Logs** page, click **Refresh**

Working with trace messages

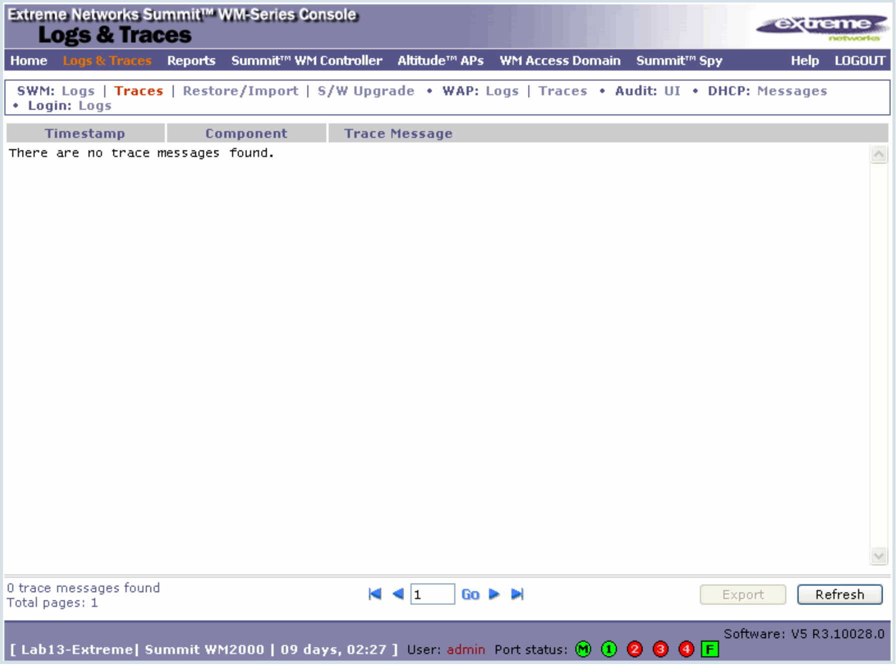
The trace messages are divided into two groups:

- Summit WM Controller trace
- Altitude AP traces

Viewing Summit WM Controller traces

To view Summit WM Controller traces:

1. From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.
2. Click the **SWM: Traces** tab. The Summit WM Controller trace page is displayed and the events are displayed in chronological order:


Extreme Networks Summit™ WM-Series Console
Logs & Traces
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
Timestamp
Component
Trace Message
Go
Export
Refresh

There are no trace messages found.

0 trace messages found
Total pages: 1

Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 02:27] User: admin Port status: M 1 2 3 4 F

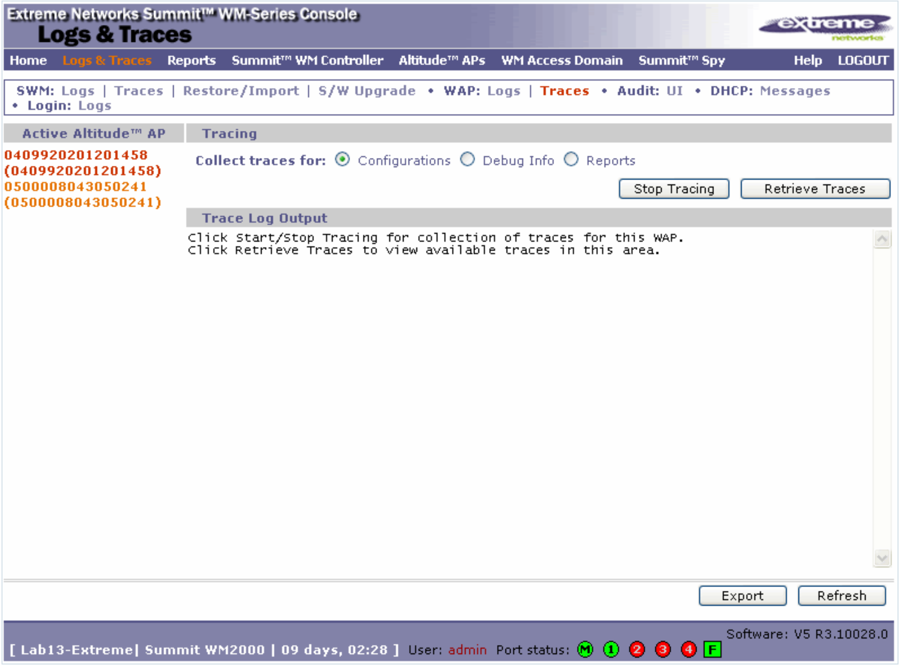
3. To sort the events by **Timestamp** or **Component**, click the appropriate column heading.
4. To refresh the Summit WM Controller trace page, click **Refresh**.
5. To export the Summit WM Controller trace page, click **Export**. The **File Download** dialog is displayed.
6. Do one of the following:
   - To open the trace file, click **Open**.
   - To save the trace file, click **Save**, and then navigate to the directory location you want to save the file.
   - Click **Save**.

Viewing Altitude AP traces

To view Altitude AP traces:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **WAP: Traces** tab. The Altitude AP trace page is displayed.



0409920201201458
(0409920201201458)
0500008043050241
(0500008043050241)

Collect traces for: ● Configurations ○ Debug Info ○ Reports

```
Click Start/Stop Tracing for collection of traces for this WAP.
Click Retrieve Traces to view available traces in this area.
```

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 02:28] User: admin Port status: M 1 2 3 4 F

CAUTION

*In order for the **Debug Info** option on the **Altitude AP Traces** page to return trace messages, this option must enabled while Altitude AP debug commands are running. To do so, you need to run a Altitude AP CLI command to turn on a specific Altitude AP debug. Once the CLI command is run, select the **Debug Info** option, and then click **Retrieve Traces**. For more information, see the Summit WM CLI Reference Guide.*

Because Altitude AP debugging can affect the normal operation of Altitude AP service, enabling debugging is not recommended unless specific instructions are provided.

3 In the **Active Altitude AP** list, click the Altitude 802.11n AP whose trace messages you want to view.

4 In the **Collect traces for** section, do the following:

- **Configurations** – Select to collect trace configuration information.
- **Start/Stop Tracing** – Click to start or stop the collection of traces for this Altitude AP.
- **Retrieve Traces** – Click to view the available configuration traces in the **Trace Log Output** section.
- **Debug info** – Select to collect trace debug information for this Altitude AP.
- **Start/Stop Tracing** – Click to start or stop the collection of traces for this Altitude AP.
- **Retrieve Traces** – Click to view the available debug traces in the **Trace Log Output** section.
- **Reports** – Select to view available crash files.
- **Retrieve Traces** – Click to view available crash files in the **Trace Log Output** section.
- **Delete all crash reports** – Click to delete all crash reports for this Altitude AP.

5 To refresh the Summit WM Controller trace page, click **Refresh**.

6 To export and view the Altitude AP trace page in HTML format, click **Export**.

Viewing Altitude 802.11n AP traces

Altitude 802.11n AP traces are combined into a single .tar.gz file and can only be viewed by saving the tar.gz file to a directory on your computer.

To view Altitude 802.11n AP traces:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **WAP Traces** tab. The Altitude AP trace page is displayed.

3 In the **Active Altitude AP** list, click the Altitude 802.11n AP whose trace messages you want to view.

4 Click **Retrieve Traces**. The **File Download** dialog appears.

5 Click **Save** and navigate to the location on your computer that you want to save the Altitude 802.11n AP trace report. The file is saved as a .tar.gz file.

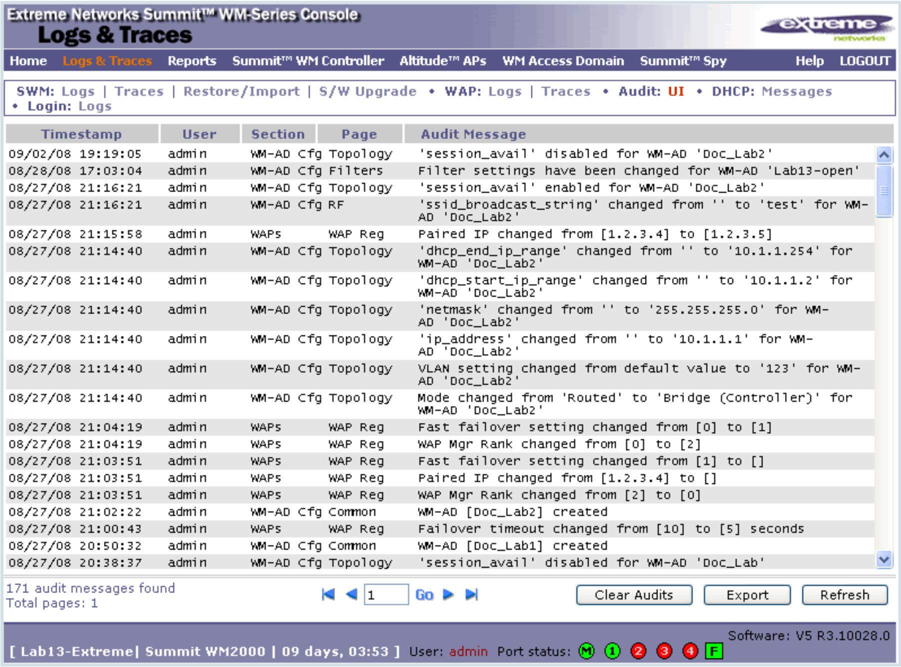
6 To view the file, unzip the .tar.gz file.

Viewing audit messages

To view audits:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **Audit: UI** tab. The audit page is displayed and the events are displayed in chronological order.



Timestamp	User	Section	Page	Audit Message
09/02/08 19:19:05	admin	WM-AD Cfg	Topology	'session_avail' disabled for WM-AD 'Doc_Lab2'
08/28/08 17:03:04	admin	WM-AD Cfg	Filters	Filter settings have been changed for WM-AD 'Lab13-open'
08/27/08 21:16:21	admin	WM-AD Cfg	Topology	'session_avail' enabled for WM-AD 'Doc_Lab2'
08/27/08 21:16:21	admin	WM-AD Cfg	RF	'ssid_broadcast_string' changed from '' to 'test' for WM-AD 'Doc_Lab2'
08/27/08 21:15:58	admin	WAPs	WAP Reg	Paired IP changed from [1.2.3.4] to [1.2.3.5]
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	'dhcp_end_ip_range' changed from '' to '10.1.1.254' for WM-AD 'Doc_Lab2'
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	'dhcp_start_ip_range' changed from '' to '10.1.1.2' for WM-AD 'Doc_Lab2'
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	'netmask' changed from '' to '255.255.255.0' for WM-AD 'Doc_Lab2'
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	'ip_address' changed from '' to '10.1.1.1' for WM-AD 'Doc_Lab2'
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	VLAN setting changed from default value to '123' for WM-AD 'Doc_Lab2'
08/27/08 21:14:40	admin	WM-AD Cfg	Topology	Mode changed from 'Routed' to 'Bridge (Controller)' for WM-AD 'Doc_Lab2'
08/27/08 21:04:19	admin	WAPs	WAP Reg	Fast failover setting changed from [0] to [1]
08/27/08 21:04:19	admin	WAPs	WAP Reg	WAP Mgr Rank changed from [0] to [2]
08/27/08 21:03:51	admin	WAPs	WAP Reg	Fast failover setting changed from [1] to []
08/27/08 21:03:51	admin	WAPs	WAP Reg	Paired IP changed from [1.2.3.4] to []
08/27/08 21:03:51	admin	WAPs	WAP Reg	WAP Mgr Rank changed from [2] to [0]
08/27/08 21:02:22	admin	WM-AD Cfg	Common	WM-AD [Doc_Lab2] created
08/27/08 21:00:43	admin	WAPs	WAP Reg	Failover timeout changed from [10] to [5] seconds
08/27/08 20:50:32	admin	WM-AD Cfg	Common	WM-AD [Doc_Lab1] created
08/27/08 20:38:37	admin	WM-AD Cfg	Topology	'session_avail' disabled for WM-AD 'Doc_Lab'

171 audit messages found
Total pages: 1

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 03:53] User: admin Port status: Ⓜ ① ② ③ ④ F

3 To sort the events by **Timestamp**, **User**, **Section**, or **Page**, click the appropriate column heading.

4 To refresh the audit page, click **Refresh**.

5 To export the audit page, click **Export**. The **File Download** dialog is displayed.

6 Do one of the following:

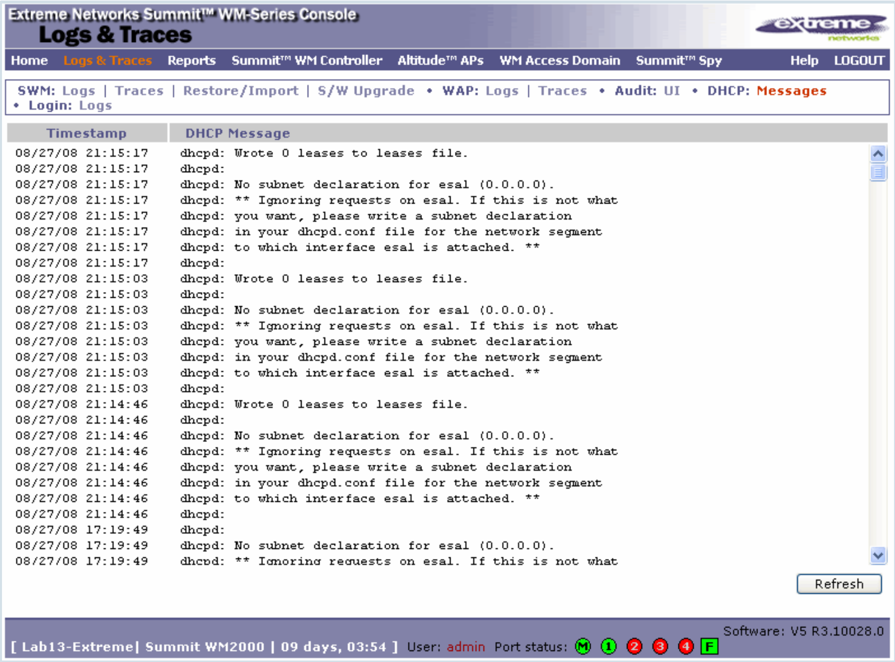
- To open the audit file, click **Open**.
- To save the audit file, click **Save**, and then navigate to the directory location you want to save the file.
- Click **Save**.

Viewing DHCP messages

To view DHCP messages:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **DHCP: Messages** tab. The DHCP message page is displayed and the events are displayed in chronological order.



```
Timestamp            DHCP Message
08/27/08 21:15:17    dhcpd: Wrote 0 leases to leases file.
08/27/08 21:15:17    dhcpd:
08/27/08 21:15:17    dhcpd: No subnet declaration for esal (0.0.0.0).
08/27/08 21:15:17    dhcpd: ** Ignoring requests on esal. If this is not what
08/27/08 21:15:17    dhcpd: you want, please write a subnet declaration
08/27/08 21:15:17    dhcpd: in your dhcpd.conf file for the network segment
08/27/08 21:15:17    dhcpd: to which interface esal is attached. **
08/27/08 21:15:17    dhcpd:
08/27/08 21:15:03    dhcpd: Wrote 0 leases to leases file.
08/27/08 21:15:03    dhcpd:
08/27/08 21:15:03    dhcpd: No subnet declaration for esal (0.0.0.0).
08/27/08 21:15:03    dhcpd: ** Ignoring requests on esal. If this is not what
08/27/08 21:15:03    dhcpd: you want, please write a subnet declaration
08/27/08 21:15:03    dhcpd: in your dhcpd.conf file for the network segment
08/27/08 21:15:03    dhcpd: to which interface esal is attached. **
08/27/08 21:15:03    dhcpd:
08/27/08 21:14:46    dhcpd: Wrote 0 leases to leases file.
08/27/08 21:14:46    dhcpd:
08/27/08 21:14:46    dhcpd: No subnet declaration for esal (0.0.0.0).
08/27/08 21:14:46    dhcpd: ** Ignoring requests on esal. If this is not what
08/27/08 21:14:46    dhcpd: you want, please write a subnet declaration
08/27/08 21:14:46    dhcpd: in your dhcpd.conf file for the network segment
08/27/08 21:14:46    dhcpd: to which interface esal is attached. **
08/27/08 21:14:46    dhcpd:
08/27/08 17:19:49    dhcpd:
08/27/08 17:19:49    dhcpd: No subnet declaration for esal (0.0.0.0).
08/27/08 17:19:49    dhcpd: ** Ignoring requests on esal. If this is not what
```

```
Software: V5 R3.10028.0
[ Lab13-Extreme| Summit WM2000 | 09 days, 03:54 ] User: admin Port status:
```

3 To sort the events by timestamp, click **Timestamp**.

4 To refresh the DHCP message page, click **Refresh**.

Viewing software upgrade and operating system patch messages

The **S/W Upgrade** tab displays the most recent upgrade actions, either success or failure, and the operating system patch history.

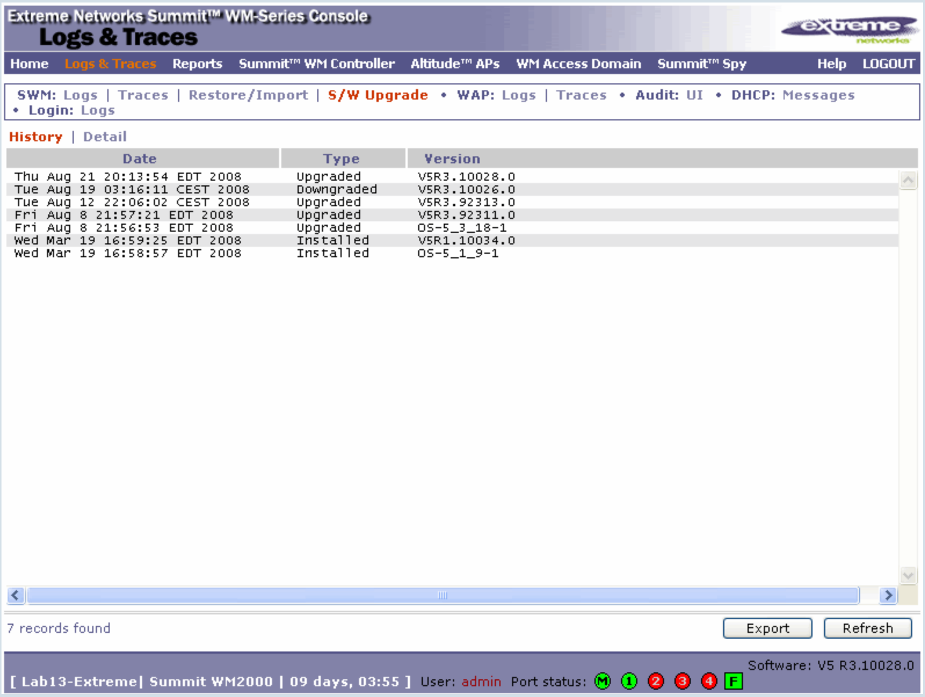
Some examples of the upgrade actions that can be displayed are:

- FTP failure during backup system image
- Database reset failure
- Database export failure
- Database import details

To view software upgrade messages:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **S/W Upgrade** tab. The software upgrade message page is displayed.


Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages • Login: Logs
History | Detail
Export
Refresh

Date	Type	Version
Thu Aug 21 20:13:54 EDT 2008	Upgraded	V5R3.10028.0
Tue Aug 19 03:16:11 CEST 2008	Downgraded	V5R3.10026.0
Tue Aug 12 22:06:02 CEST 2008	Upgraded	V5R3.92313.0
Fri Aug 8 21:57:21 EDT 2008	Upgraded	V5R3.92311.0
Fri Aug 8 21:56:53 EDT 2008	Upgraded	OS-5_3_18-1
Wed Mar 19 16:59:25 EDT 2008	Installed	V5R1.10034.0
Wed Mar 19 16:58:57 EDT 2008	Installed	OS-5_1_9-1

7 records found

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 03:55] User: admin Port status: Ⓜ ① ② ③ ④ F

3 Do the following:

- To view software upgrade messages, click **Detail**.
- To view the operating system history, click **History**.

4 To refresh the page, click **Refresh**.

5 To export the software upgrade messages or operating system history, click **Export**. The **File Download** dialog is displayed.

6 Do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, and then navigate to the directory location you want to save the file.
- Click **Save**.

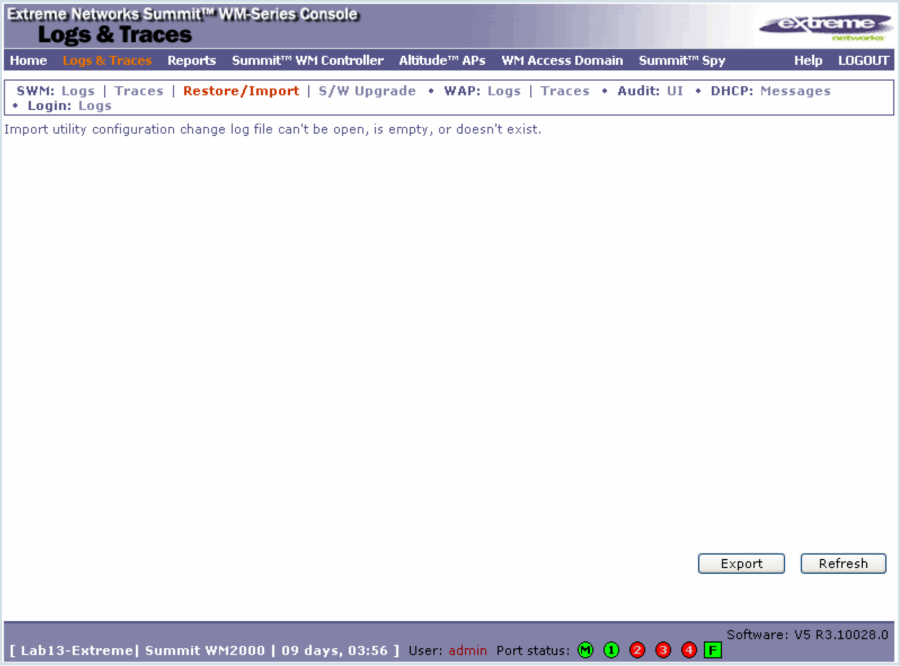
Viewing restore/import messages

The **Restore/Import** tab displays the most recent restore/import results.

To view restore/import messages:

1 From the main menu, click **Logs & Traces**. The **Logs & Traces** page is displayed.

2 Click the **Restore/Import** tab. The restore/import message page is displayed.


Extreme Networks Summit™ WM-Series Console
Logs & Traces
extreme networks
Home
Logs & Traces
Reports
Summit™ WM Controller
Altitude™ APs
WM Access Domain
Summit™ Spy
Help
LOGOUT
SWM: Logs | Traces | Restore/Import | S/W Upgrade • WAP: Logs | Traces • Audit: UI • DHCP: Messages
• Login: Logs
Export
Refresh
Software: V5 R3.10028.0
[Lab13-Extreme| Summit WM2000 | 09 days, 03:56] User: admin Port status: M 1 2 3 4 F

```
Import utility configuration change log file can't be open, is empty, or doesn't exist.
```

3 To refresh the restore/import message page, click **Refresh**.

4 To export the restore/import message page, click **Export**. The **File Download** dialog is displayed.

5 Do one of the following:

- To open the file, click **Open**.
- To save the file, click **Save**, and then navigate to the directory location you want to save the file.
- Click **Save**.

8 Summit WM Controller's utilities

The topics in this chapter are organized as follows:

- Using controller utilities
- Configuring Check Point event logging
- Enabling SNMP

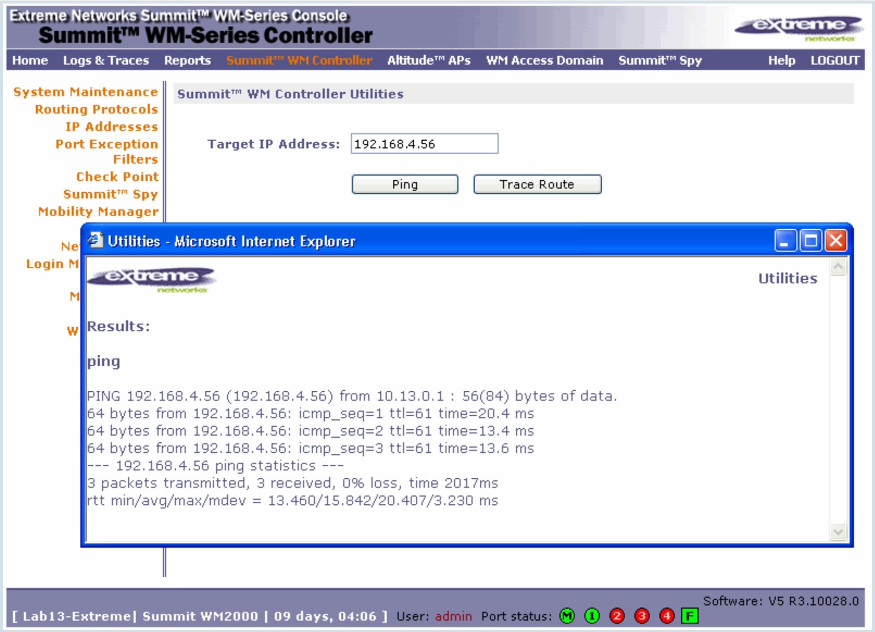
Using controller utilities

You can use Summit WM Controller utilities to test a connection to the target IP address and record the route through the Internet between your computer and the target IP address. In addition, you can also use Summit WM Controller utilities to capture exception traffic, which can be useful for network administrators when debugging network problems.

To test or record IP address connections:

1. From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.
2. In the left pane, click **Utilities**. The **Summit WM Controller Utilities** page is displayed.
3. In the **Target IP Address** box, type the IP address of the destination computer.
4. To test a connection to the target IP address, click **Ping**. A pop-up window is displayed with the ping results.

   The following is an example of ping results.



Target IP Address: 192.168.4.56

Results:

ping

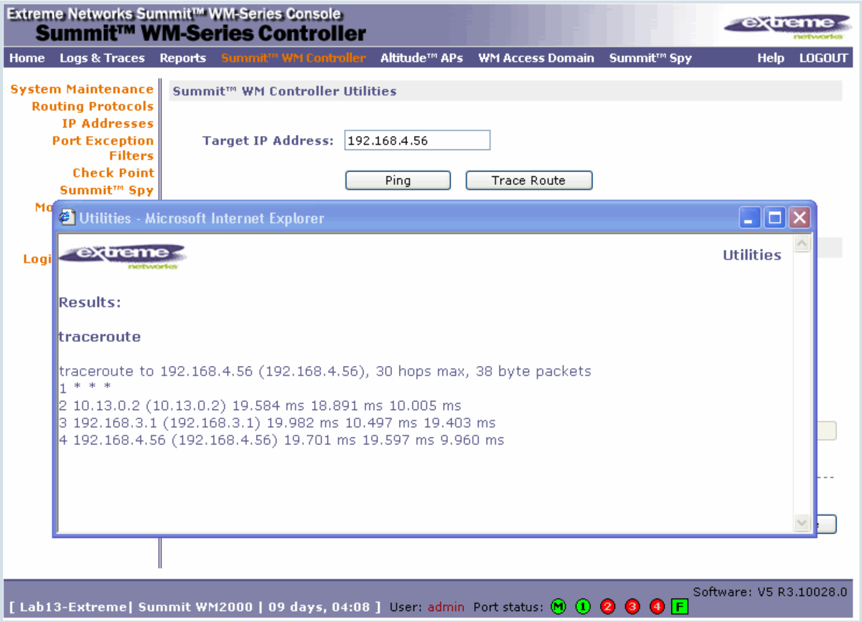
```
PING 192.168.4.56 (192.168.4.56) from 10.13.0.1 : 56(84) bytes of data.
64 bytes from 192.168.4.56: icmp_seq=1 ttl=61 time=20.4 ms
64 bytes from 192.168.4.56: icmp_seq=2 ttl=61 time=13.4 ms
64 bytes from 192.168.4.56: icmp_seq=3 ttl=61 time=13.6 ms
--- 192.168.4.56 ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2017ms
rtt min/avg/max/mdev = 13.460/15.842/20.407/3.230 ms
```

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 04:06] User: admin Port status: M 1 2 3 4 F

5. To record the route through the Internet between your computer and the target IP address, click **Trace Route**.

The following is an example of trace results.



Target IP Address: 192.168.4.56

Results:

traceroute

```
traceroute to 192.168.4.56 (192.168.4.56), 30 hops max, 38 byte packets
1 * * *
2 10.13.0.2 (10.13.0.2) 19.584 ms 18.891 ms 10.005 ms
3 192.168.3.1 (192.168.3.1) 19.982 ms 10.497 ms 19.403 ms
4 192.168.4.56 (192.168.4.56) 19.701 ms 19.597 ms 9.960 ms
```

[Lab13-Extreme| Summit WM2000 | 09 days, 04:08] User: admin Port status: M 1 2 3 4 F

Software: V5 R3.10028.0

Summit WM Controller TCP dump management

Summit WM Controller TCP dump management allows you to capture exception traffic that is sent to the management plane. Exception traffic is defined as traffic that is sent to the management plane from the data/control plane for special handling. For example, exception traffic can include DHCP, OSPF, and TFTP traffic.

When capturing exception traffic, you define the following:

- The physical or virtual WM-AD port on which the captured exception traffic travels
- The name and size of the captured traffic file
  - When naming the file, the file name extension must be .cap.
  - 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.
- The location where the captured TCP dump file is saved

NOTE

Only the Summit WM200/2000 Controller provides the option of defining the location, where the captured TCP dump file is saved.

The captured traffic file is stored in a binary tcpdump-format file on the Summit WM Controller or compact flash card. The captured traffic file can then be exported to a local machine for packet analysis and opened with a traffic analysis tool. For example, Wireshark.

Summit WM Controller can only store one captured traffic file. If you choose to save the captured traffic file on a compact flash card, the available space on the compact flash card will dictate how many captured traffic files you can save.

NOTE

Only the Summit WM200/2000 Controller give you the option of saving the TCP dump file on the CF card. The other platforms do not support the CF card.

To capture exception traffic:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 In the left pane, click **Utilities**. The **Summit WM Controller Utilities** page is displayed.

3 In the **Tcpdump Management Port** drop-down list, click the port on which the exception traffic travels that you want to capture.

4 In the **Filename** box, type the name for the captured traffic file. The default name is **mgmt_traffic_dump.cap**.

5 In the **Capture File Size(MB)** box, type the maximum size for the captured traffic file. 10 MB is the minimum and 1 GB is the maximum size of the captured traffic file.

NOTE

If you are using any of the following platforms, you must skip Step 6.
• Summit WM100 Controller
• Summit WM1000 Controller
• Summit WM20 Controller

6 In the **Destination** drop-down list, do one of the following:

- **Flash –** Click to save the file on the flash card.
- **Local –** Click to save the file locally on the Summit WM Controller.

NOTE

*The **Destination** drop-down list is only available if the Summit WM Controller has a mounted flash card. For more information, see "Working with a CF card" on page 55.*

NOTE

Only the Summit WM200/2000 Controller supports the CF card.

7 Click **Start**. A dialog is displayed informing you the previously captured file will be removed.

8 To continue with the exception traffic capture, click **OK**. A dialog is displayed informing you the capture has started.

- In applicable, to stop the capture before it is completed, click **Stop**.

To export an exception traffic capture file:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 In the left pane, click **Utilities**. The **Summit WM Controller Utilities** page is displayed.

3 In the **Capture Files on System** drop-down list, click the capture file you want to export, and then click **Export**. A **File Download** dialog is displayed asking you where you want to save the file.

4 Click **Save**.

Navigate to the location on your network that you want to save the file, and then click **Save**.

Configuring Check Point event logging

The Summit WM Controller can forward specified event messages to an ELA server using the OPSEC ELA protocol - Event Logging API (Application Program Interface). On the ELA server, the event messages are tracked and analyzed, so suspicious messages can be forwarded to a firewall application that can take corrective action.

Check Point created the OPSEC (Open Platform for Security) alliance program for security application and appliance vendors to enable an open industry-wide framework for inter operability.

When ELA is enabled on the Summit WM Controller, it forwards the specified event messages from its internal event server to the designated ELA Management Station on the enterprise network.

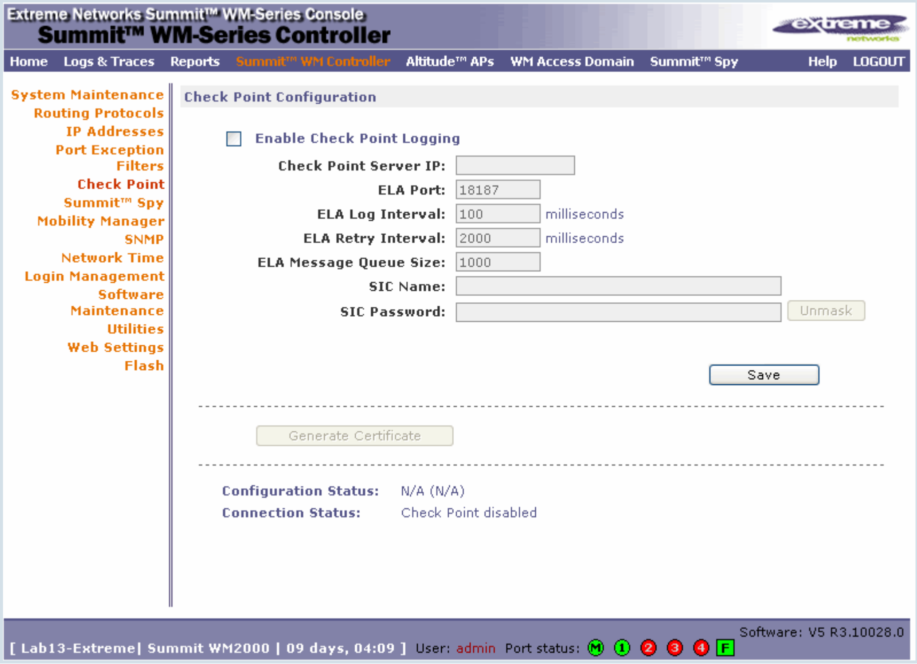
NOTE

Before you set up the Summit WM Controller, you must first create OPSEC objects for Summit WM Controller in the Check Point management software. The name and password you define must also be entered into the ***Check Point Configuration*** *page.*

To enable and configure Check Point:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 In the left pane, click **Check Point**. The **Check Point Configuration** page is displayed.



Check Point Configuration

□ Enable Check Point Logging

Check Point Server IP:

ELA Port: 18187

ELA Log Interval: 100 milliseconds

ELA Retry Interval: 2000 milliseconds

ELA Message Queue Size: 1000

SIC Name:

SIC Password:

Configuration Status: N/A (N/A)

Connection Status: Check Point disabled

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 04:09] User: admin Port status: M 1 2 3 4 F

3 To enable check point logging, select the **Enable Check Point Logging** checkbox.

4 Type the following information:

- **Check Point Server IP** – Specifies the IP address of the ELA Management Station
- **ELA Port** – Specifies the port to use for ELA. The default port is 18187.
- **ELA Log Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting to log once there is a connection between Summit WM Controller and the Check Point gateway. The default is **100** milliseconds.
- **ELA Retry Interval** – Specifies the amount of time (in milliseconds) you want the system to wait before attempting a re-connection between Summit WM Controller and the Check Point gateway. The default is **2000** milliseconds.
- **ELA Message Queue Size** – Specifies the number of messages the log queue holds if the Summit WM Controller and the Check Point gateway become disconnected. The default is **1000** log entries.
- **SIC Name** – Specifies the Secure Internal Communication (SIC) Name, your security-based ID.
- **SIC Password** – Specifies your Secure Internal Communication (SIC) password. You can use the **Unmask** button to display the password.

5 To save your changes, click **Save**.

6 To create the certificate to be sent to the ELA Management Station, click **Generate Certificate**.

If the certificate is properly generated and the connection with the ELA Management Station is made, the **Connection Status** section displays the following message:

OPSEC Connection OK

If there is an error in generating the certificate or establishing the connection, the **Connection Status** section displays the following message:

OPSEC Connection Error

ELA Management Station events

The events for the ELA Management Station are grouped under Extreme and are mapped as info events and alert events. The alerts include:

- Altitude AP registration and/or authentication failed
- Authentication User Request unsuccessful
- RADIUS server rejected login (Access Rejected)
- An unknown AP has attempted to connect. AP authentication failure.
- A connection request failed to authenticate with the CM messaging server. This may indicate port-scanning of the Summit WM Controller, or a back-door access attempt.
- Unauthorized client attempting to connect

Enabling SNMP

The Summit WM software system supports Simple Network Management Protocol (SNMP), Version 1 and 2c. SNMP, a set of protocols for managing complex networks, is used to retrieve Summit WM Controller statistics and configuration information.

SNMP sends messages, called protocol data units (PDUs), to different parts of a network. Devices on the network that are SNMP-compliant, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

NOTE

In this current release (V5R3), the SNMP protocol does not support the Altitude 802.11n AP since some of the Altitude 802.11n AP properties are not accurately reported.

MIB support

The Summit WM software system accepts SNMP Get commands and generates Trap messages. Support is provided for the retrieval information from the router MIB-II (SNMP_GET) as well as SNMP traps. The supported MIBs include:

- SNMPv2-MIB
- IF-MIB
- IEEE802dot11-MIB
- RFC1213-MIB

NOTE

The Summit WM Controller is not fully compliant with MIB II. For example, esa/IXP ports only provide interface statistics.

The **Extreme Networks Enterprise MIB** includes:

- EXTREME-SUMMIT-WM-MIB
- EXTREME-SUMMIT-WM-PRODUCTS-MIB
- EXTREME-SUMMIT-WM-SMI.my
- EXTREME-SUMMIT-WM-DOT11-EXTNS-MIB
- EXTREME-SUMMIT-WM-BRANCH-OFFICE-MIB

The MIB is provided for compilation into an external NMS. No support has been provided for automatic device discovery by an external NMS.

The Summit WM Controller is the only point of SNMP access for the entire system. In effect, the Summit WM Controller proxies sets, gets, and alarms from the associated Altitude APs.

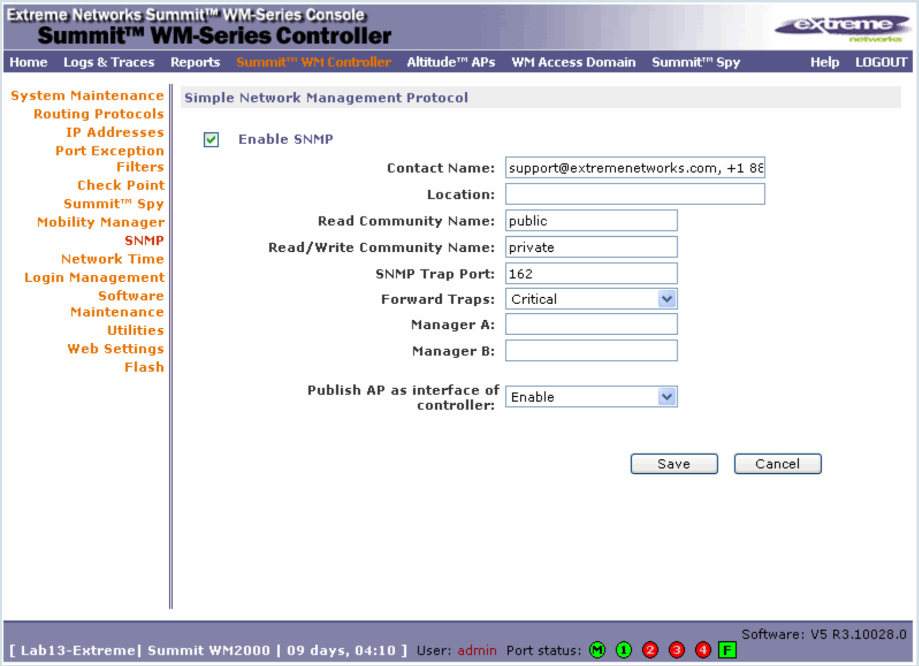
Enabling SNMP on the Summit WM Controller

You can enable SNMP on the Summit WM Controller to retrieve statistics and configuration information.

To enable SNMP Parameters:

1 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.

2 In the left pane, click **SNMP**. The **Simple Network Management Protocol** page is displayed.



Simple Network Management Protocol

☑ Enable SNMP

Contact Name: support@extremenetworks.com, +1 88

Location:

Read Community Name: public

Read/Write Community Name: private

SNMP Trap Port: 162

Forward Traps: Critical

Manager A:

Manager B:

Publish AP as interface of controller: Enable

3 Type the following:

- **Contact Name** – Specifies the name of SNMP administrator.
- **Location** – Specifies the location of the SNMP administration machine.
- **Read Community Name** – Specifies the community name for users with read privileges.
- **Read/Write Community Name** – Specifies the community name for users with read and write privileges.
- **SNMP Trap Port** – Specifies the destination port for SNMP traps. The industry standard is 162. If left blank, no traps are generated.
- **Forward Traps** – Specifies the security level of the traps to be forwarded. From the drop-down list, click **Informational**, **Minor**, **Major**, or **Critical**.
- **Manager A** – Specifies the IP address of the specific machine on the network where the SNMP traps are monitored.
- **Manager B** – Specifies the IP address of a second machine on the network where the SNMP traps are monitored, if Manager A is not available.

NOTE

For security purposes, it is recommended that you immediately change the Read Community Name (public) and the Read/Write Community Name (private) to names that are less obvious and more secure.

NOTE

If you are using any of the following Summit WM Controllers, you must skip Step 4.
• Summit WM100 Controller
• Summit WM1000 Controller

4 In the **Publish AP as interface of controller** drop-down list, click whether to enable or disable publishing the Altitude AP and their interfaces as interfaces of the Summit WM Controller. By default this option is enabled.

When this option is enabled, all Altitude APs and their interfaces are published as interfaces of the Summit WM Controller when you retrieve topology statistics and configuration information using the SNMP protocol.

Topology statistics and configuration information on Altitude APs are retrievable using both proprietary and standard MIB. The **Publish AP as interface of controller** option only affects information retrieved through standard MIB, i.e. IF-MIB, RFC1213. All information that is retrieved through proprietary MIB is not affected. If the **Publish AP as interface of controller** option is disabled, the Altitude APs' interfaces are not considered interfaces of the Summit WM Controller.

For example, if the **Publish AP as interface of controller** option is disabled, querying the ifTable would return information on the Summit WM Controller physical interfaces, plus all WM-ADs that are configured on that controller. If enabled, querying the same table would return the above information, in addition to information on each Altitude APs’ interfaces.

NOTE

*The **Publish AP as interface of controller** feature is supported only by the following Summit WM Controller:*
• Summit WM200/2000 Controller
• Summit WM20 Controller

5 To save your changes, click **Save**.

9 Recovering the Summit WM Controller’s lost password

The Summit WM Software enables you to recover the Summit WM Controller via the **Rescue** mode if you have lost its login password.

The **Rescue** mode provides the following options via its **Authentication Service Management Menu** to recover the Summit WM Controller:

- **Set Login Mode to Local** — Use this option if the login authentication mode was set to RADIUS-based authentication, and you want to revert to the local login authentication mode.
- **Reset Accounts and Passwords to Factory Default** — Use this option if you want to reset the login accounts and password to factory defaults.
- **Change administrator password** — Use this option if you want to change the administrator’s password.

NOTE

You must use the serial connection to Summit WM Controller to recover its lost login password.

NOTE

The procedure starts with a reboot.

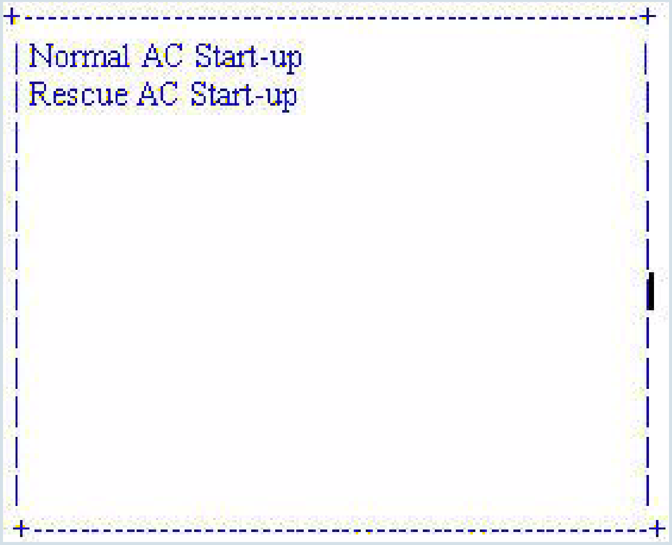
Recovering the WM100/1000 Controller’s lost password

To recover the WM100/1000 Controller’s lost login password:

1 Use the serial port of the WM100/1000 Controller to connect to the console.

> **NOTE**
>
> *To enter the **Rescue** mode, you must connect to the serial port. You can not enter the **Rescue** mode by connecting to the ESA ports, or management/ETH0 port.*

2 Reboot the Summit WM Controller. The following menu appears during the reboot process.



```
Normal AC Start-up
Rescue AC Start-up
```

3 Select **Rescue AC Start-up** and then press **Enter**. The **Rescue** menu appears.

NOTE

Use the ***^*** *and* ***v*** *keys on your keyboard to select the entries in the above menu.*

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force System Recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image directly from the FTP server
   8) Authentication Service Management Menu

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the image
installed at the factory.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice:
```

4 Type 8. The **Authentication Service Management** menu appears.

```
Authentication Service Management Menu
   ======================================
   1) Set Login Mode to Local
   2) Reset Accounts and Passwords to Factory Default
   3) Change administrator password
   4) Return to main menu
Please enter your choice:
```

5 Type the sequence number of the appropriate option, given in the **Authentication Service Management** menu.

- **Set Login Mode to Local** — Type **1** if the login authentication mode was set to RADIUS-based authentication, and you want to revert to the local login authentication mode.
- **Reset Accounts and Passwords to Factory Default** — Type **2** if you want to reset the login accounts and password to factory defaults.
- **Change administrator password** — Type **3** if you want to change the administrator's password.
- **Return to main menu** — Type **4** if you want to return to the main menu.

6 After you have used any of the first three options in the **Authentication Service Management** menu, press **Enter** to return to the main menu.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force System Recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image directly from the FTP server
   8) Authentication Service Management Menu

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall
the image installed at the factory.

Reboot will restart the system back into Normal mode.
```

7 Type **9**. The system restarts into normal mode.

Recovering the WM20/200/2000 Controller's lost password

To recover the WM20/200/2000 Controller's lost login password:

1 Use the serial port of the WM200/2000/100 Controller to connect to the console.

NOTE

*To enter the **Rescue** mode, you must connect to the serial port. You can not enter the **Rescue** mode by connecting to the ESA ports, or management/ETHO port.*

2 Reboot the Summit WM Controller. The following menu appears during the reboot process.

```
---------------------------------------------------------------
0: Main Mode
1: Rescue Mode
---------------------------------------------------------------
   Use the number 0 and 1 keys to select which entry is highlighted.
   Press enter to boot the selected OS, 'e' to edit the
   commands before booting, or 'c' for a command-line.
   Highlighted entry is 0:
```

3 Select the **Rescue Mode**, and then press **Enter**. The **Rescue Start-up Menu** appears.

```
Rescue Start-up Menu. Use with extreme caution.
   1) Force system recovery
   2) Configure interface
   3) Configure ftp settings
   4) Network settings Menu
   5) FTP settings Menu
   6) Create backup
   7) Flash Menu
   8) Authentication Service Management Menu

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall the backup
image.
Reboot will restart the system back into Normal mode.
If you have any questions about these options, please contact Support.
Your choice>
```

4 Type **8**. The **Authentication Service Management** menu appears.

```
Authentication Service Management Menu
   ======================================
   1) Set Login Mode to Local
   2) Reset Accounts and Passwords to Factory Default
   3) Change administrator password
   4) Return to main menu
Please enter your choice:
```

5 Type the sequence number of the appropriate option, given in the **Authentication Service Management** menu.

- **Set Login Mode to Local** — Type **1** if the login authentication mode was set to RADIUS-based authentication, and you want to revert to the local login authentication mode.
- **Reset Accounts and Passwords to Factory Default** — Type **2** if you want to reset the login accounts and password to factory defaults.
- **Change administrator password** — Type **3** if you want to change the administrator's password.
- **Return to main menu** — Type **4** if you want to return to the main menu.

6 After you have used any of the first three options in the **Authentication Service Management** menu, press **Enter** to return to the main menu.

```
Rescue AC Start-up Menu. Use with extreme caution.
   1) Force System Recovery
   2) Create System Backup Image
   3) Display Backup Images
   4) FTP Menu
   5) Network Interface Menu
   6) Manually run File System Check Utility (fsck)
   7) Restore Backup Image directly from the FTP server
   8) Authentication Service Management Menu

   9) Reboot
WARNING! - Forcing system recovery will erase all files, and reinstall
the image installed at the factory.

Reboot will restart the system back into Normal mode.
```

7 Type **9**. The system restarts into normal mode.

10 Maintaining the Summit WM Controller

This chapter describes how to maintain the important components of the following Summit WM Controllers.

- Summit WM200/2000 Controller
- Summit WM20 Controller

The topics in this chapter are organized as follows:

- Maintaining the Summit WM200/2000 Controller
- Maintaining the Summit WM20 Controller

Maintaining the Summit WM200/2000 Controller

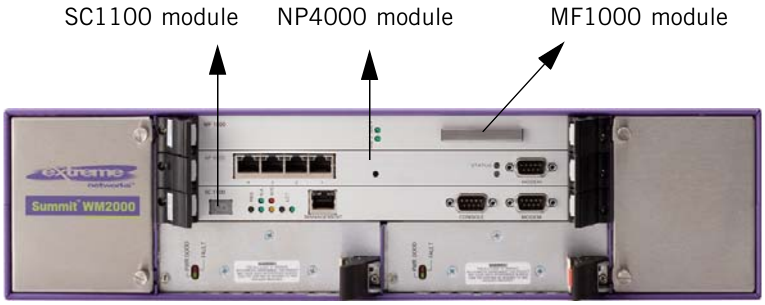
WARNING!

The Summit WM200/2000 Controller should not be operated in a LAN wherein a DC voltage is overlaid on the data lines, since there may be switches that still connect directly without checking the supply voltage. Depending on the transformer at the LAN interface, voltages of up to 500 V can be induced. Such peak voltages usually lead to destruction of the physical LAN controller's logic.

The Summit WM200/2000 Controller consists of a cassette with a cPCI backplane, NP4000 Blade, MF1000 card, Blade module, SC1100 module, power supply unit and redundant fan modules. Depending on the power supply module used, it can operate with either 110 or 230V AC.

There is no electrical connection between the Altitude APs and the Summit WM200/2000 Controller. The Summit WM200/2000 Controller and the Altitude APs communicate with each other exclusively via the IP network. For more information, see the *Summit WM User Guide.*

Figure 10: Summit WM200/2000 Controller's front panel



WARNING!

MF1000, NP4000 and SC1100 maintenance is achieved by replacing the affected parts.
Properly shutdown the system prior to performing any maintenance on the system's main processing components,

including the MF1000, NP4000, and SC1100 cards. For more information, see "Powering off the Summit WM200/ 2000 Controller" on page 120.

Data ports cabling specification

The Summit WM200/2000 Controller's data ports have copper connectors.

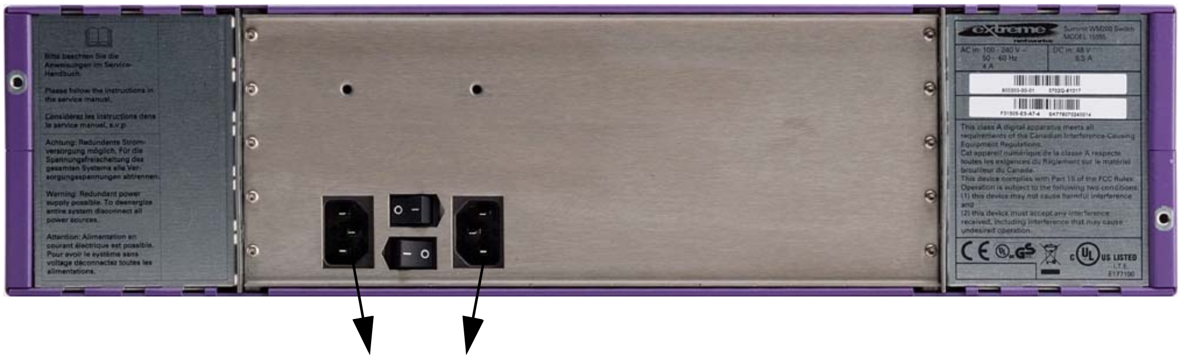
NOTE

If your infrastructure does not allow a copper connection, you must get a Gigabit Media Converter to convert the copper connection to a fibre optic connection. For example, you can use Netgear GC102 converter that receives the copper connection and outputs traffic via the fibre optic connector.

Summit WM200/2000 Controller power supply

The Summit WM200/2000 Controller is equipped with a redundant power supply. The redundant power supply provides the Summit WM200/2000 Controller with two power supplies. The duo power supplies provide administrators with the option of connecting a second power supply to an independent power source to ensure constant power availability in case of a power outage.

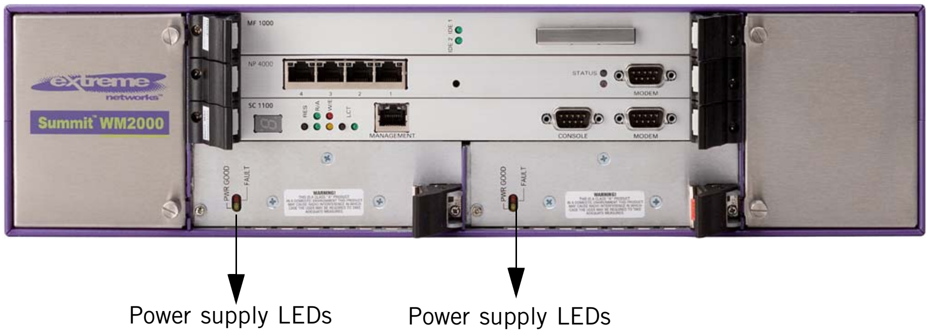
Figure 11: Summit WM200/2000 Controller power supply plugs and switches



Redundant power supply

The power supply LEDs on the front panel of the Summit WM200/2000 Controller indicate whether one power supply, or both the power supplies are connected to the power source.

Figure 12: Power supply LEDs



If a power supply is connected, the **PWR GOOD** (amber) LED is lit. If a power supply is not connected, or if the power supply is connected but is experiencing problems, the **FAULT** (red) LED is lit.

Power FRUs

This section describes the power field replaceable units (FRUs) for the Summit WM200/2000 Controller. It also provides procedures for removing, replacing, and verifying each FRU.

Summit WM200/2000 Controller, AC-powered, redundant system

The power FRUs on an AC-powered redundant Summit WM200/2000 Controller are two AC-to-DC shelf power supply units (ACPCI).

Fan Tray

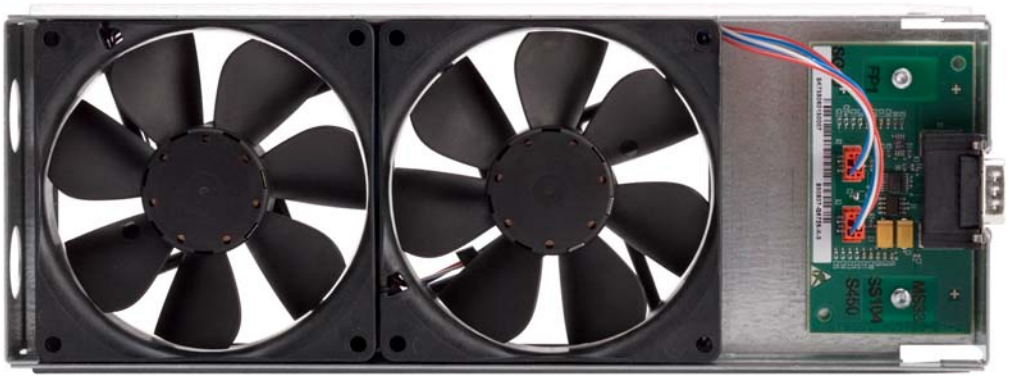
The fan tray is a plug-in unit for 19-inch houses and consists of two 12-V DC fans. It is suitable for on-site installation and replacement. An air current (from left to right) of 84 m3/h per fan is sufficient. Each fan generates a square wave, open collector signal that is proportional to the fan speed. The absence of this signal indicates a fan problem in the system. The fan tray is hot swappable. In order to replace the fan tray, the two screws on the fan tray cover must be removed.

WARNING!

Exercise caution when removing fan trays. It is recommended to wait until the fans stop rotating before removing the fan trays.

Figure 13 illustrates the fan model that is used: PAPST 3412 N/2.

Figure 13: Fan Tray



The fan trays are positioned on the left and right in the Summit WM200/2000 Controller shelf. Each fan features three conductors {12 V, ground (GND), speed signal}. The fan trays are connected to the backplane by a connection cable.

Figure 14 illustrates the fan tray covers, as well as the numbering of the fans. Figure 15 illustrates the ventilation grills for the Summit WM200/2000 Controller fans.

Figure 14: Fan tray covers and numbering of fans

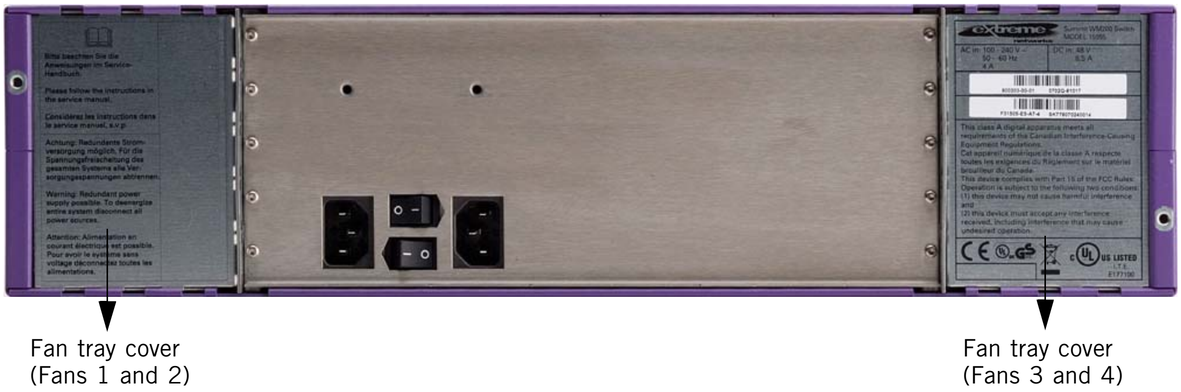
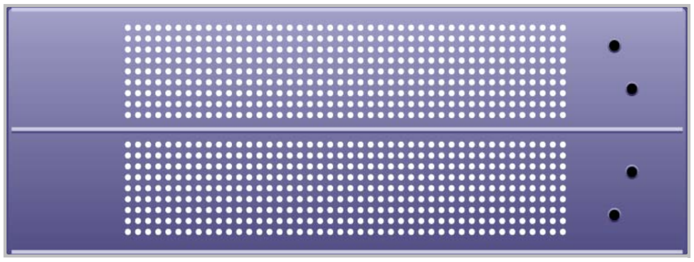


Figure 15: Summit WM200/2000 Controller ventilation grills

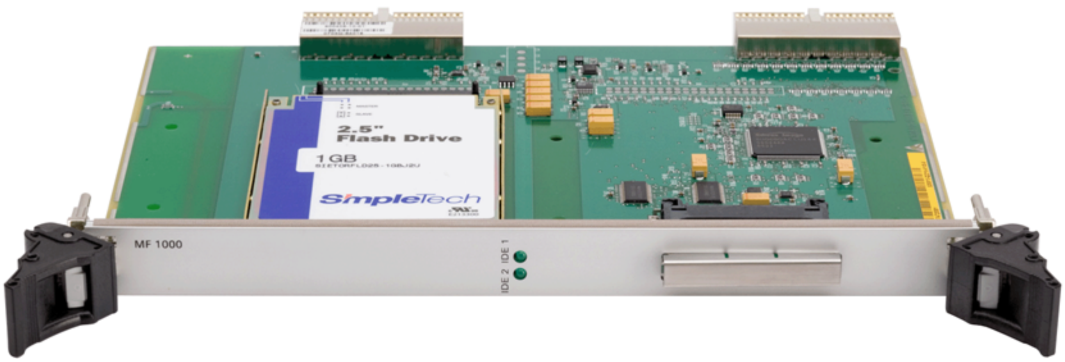


MF1000 Media Flash Card

The MF1000 card consists of a 1GB Flash Disk Drive. This card provides the persistent storage for the system. This card should not be unplugged during the live operation of the system. The system should be powered down prior to removal of the card to prevent any loss or corruption of persisted data.

Before powering down the system, the system's services should also be halted through the administration interface.

Figure 16: MF1000 card



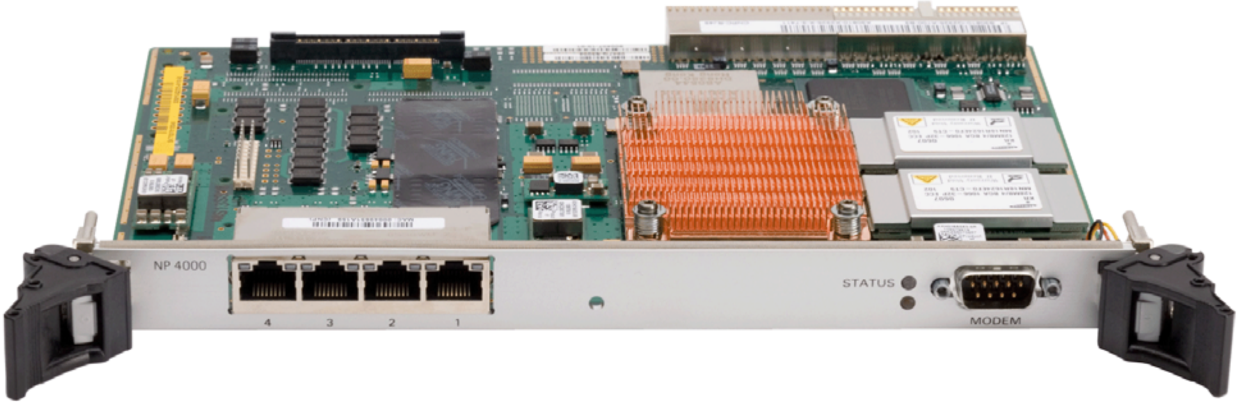
The MF1000 card includes:

- **Hardware Part Number** – MF1000 (including Flashdrive) S30810-K2319-X100
  - WM200/2000 Media Services Engine (MSE 2011)
- **LEDs** – The front side of the card features two green LEDs (IDE1 = HD/IDE2 = MO) that indicate the status of the individual drives.
- **Compact Flash** – A 1GB compact flash interface is also available on the card. The compact flash interface supports image management operations.

NP4000 Network Processor Card

The NP4000 card is a full size (6U) Compact PCI (cPCI) form-factor card.

Figure 17: NP4000 card



The NP4000 card has the following main components:

- Pentium M processor
- Micron North Bridge with dual PCI bus
- 1GB DDR memory
- Dual stage Watchdog timer
- Two signal interfaces from redundant PSU that provide the following information to CPU (registered and memory mapped):
  - Provide alarm from PSU to s/w if redundant power module failed
- 2 MB of onboard Flash (used for system Bootrom, diagnostic, system serial number, Extreme Networks-specific MAC address for Eth ports, etc…; accessible by s/w applications).
- Management ports:
  - Main: 10/100BT LAN (RJ45) with Extreme Networks-specific MAC address, activity LED (bi-color) and speed LED (bi- color).
  - Console access port: RS-232 (DB9) serial interface
- CPU card provides seven-segment LED display and four status LEDs (under s/w control) as a way to visually communicate with service personnel and end users
- One Reset button (external)

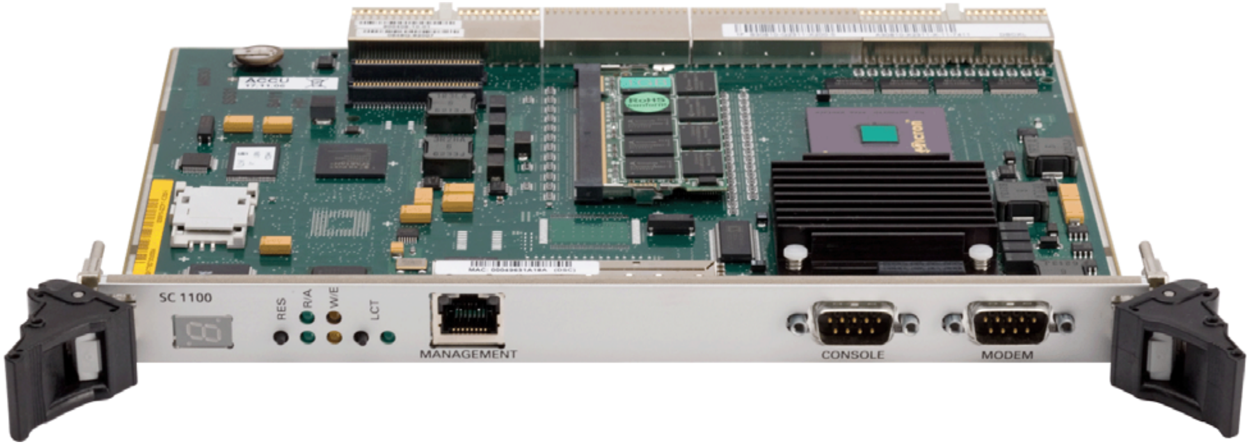
NOTE

Replacing the NP4000 blade will alter the MAC address of the management interface, which affects the product licensing system. As such, replacement of the NP4000 requires that the product key be transferred from the old NP4000 card to the new one. This transfer should be arranged through Extreme Networks technical support or sales support.

SC1100 Supervisor Card

The SC1100 card is a full size (6U) hot swappable Compact PCI (cPCI) form-factor card.

Figure 18: SC1100 card



The SC1100 card has with the following main components:

- Network processor Unit
- 256MB of RDRAM
- 32MB of QDR SSRAM
- Non-transparent PCI bridge (Intel 21555) to provide 33/66MHz 32/64-bit PCI bus connectivity between NPU PCI interface and cPCI backplane
- 12-port SPI4.2 Gigabit Mac
- 4 x front-accessible Gigabit (data) ports

NOTE

Replacing the SC1100 alters the MAC addresses of the system data ports. New MAC addresses are advertised on the network in relation to the system interface IPs. You must ensure that no specific network topology is in place which can be affected by the MAC address change to the network. The IP addresses for the system do not change.

Summit WM200/2000 Controller power and maintenance procedures

This section provides procedures to power off and power on the system when performing maintenance. Use the following information to help eliminate system problems.

Tools and equipment required

Use the following tools and equipment to power on the system and verify system power:

- ESD kit
- Phillips screwdriver

Maintaining the ESD wrist strap

The ESD wrist strap and cord must operate properly to guard against ESD damage and electrical shocks. The wrist strap and cord assembly has a 1-megohm resistor; if the resistor fails, there is no ESD protection.

NOTE

Check the wrist strap weekly to ensure proper ESD protection.

To test the ESD wrist strap using a DMM:

1 Set the ohmmeter to 2-megohm resistance (see Figure 19).

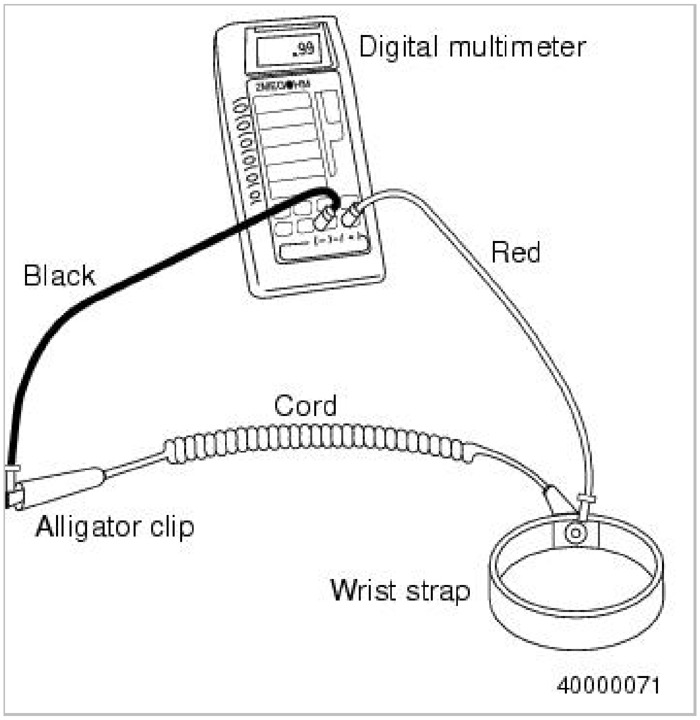
2 Connect the DMM black lead to the alligator clip at the end of the cord.

3 Contact the DMM red lead to the plate on the inner surface of the wrist strap.

4 Check the resistance reading on the meter. The meter reading must be between 0.80 and 1.20 mega ohms.

5 Replace the wrist strap and cord assembly if the reading is not within the allowable range.

Figure 19: ESD Wrist Strap and Cord Assembly



Using electrostatic discharge prevention procedures

Always follow the electrostatic discharge (ESD) prevention procedure when you remove and replace cards. Failure to follow the ESD prevention procedure can result in permanent or intermittent card failures.

CAUTION

Observe all precautions for electrostatic discharge.

WARNING!

To avoid electrical shock, never wear the ESD wrist strap while working on the power system or at the back of the cabinet.

To perform ESD prevention procedures:

1. Check the ESD wrist strap weekly to ensure proper ESD protection (refer to "Maintaining the ESD wrist strap" on page 118 and Figure 19).
2. Attach the ESD wrist strap to your bare wrist. Ensure that the inside surface of the strap makes good contact with your skin (see Figure 7-2).
3. Attach one end of the coiled wire to the wrist strap and the other end to the alligator clip if necessary.
4. Connect the alligator clip to an unpainted portion of the cabinet frame. This safely channels electrostatic charges to ground.
5. Observe the following ESD prevention guidelines during the performance of system maintenance procedures:
   - Handle cards by their edges only

     CAUTION

     Avoid contact between the card and your clothing. Electrostatic charges on clothing can damage the card. The wrist strap protects the card from electrostatic charges on your body only.

   - Immediately place any card you remove from the system into a static-shielding package.

     CAUTION

     The card must remain in a static-shielding bag or static-free box until the card is returned to the warehouse.

   - Do not remove a replacement card from its static-shielding packaging until you are ready to install it.

     NOTE

     This procedure applies to upgraded systems.

   - Remove cards by pressing/pulling the cPCI card ears

     NOTE

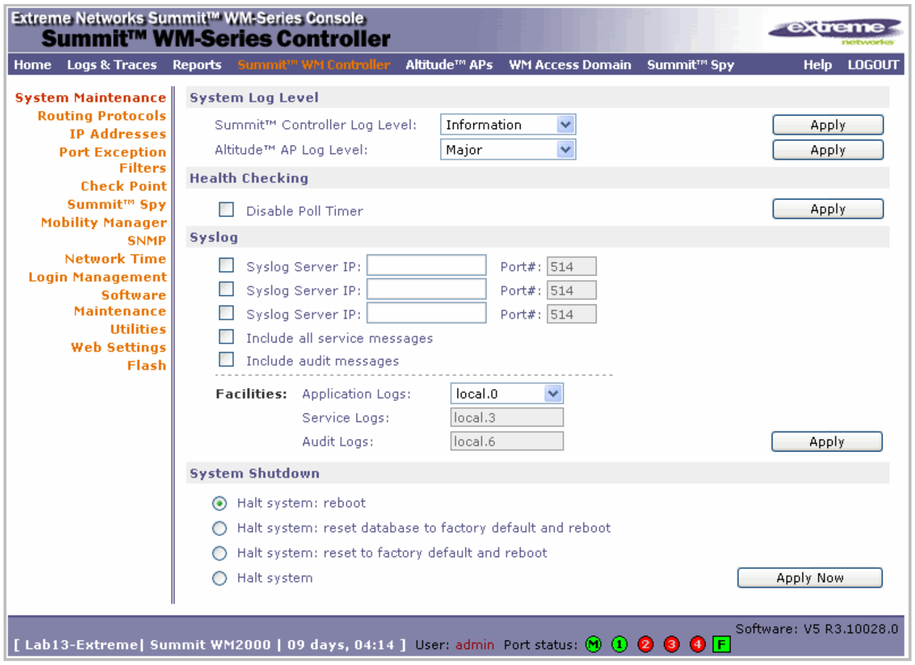
     Cards are locked from manufacturing with a screw at each end. In order to remove a card, the holding screws must be removed.

Powering off the Summit WM200/2000 Controller

To power off the Summit WM200/2000 Controller:

1 Login on the Summit WM200/2000 Controller.

2 From the main menu, click **Summit WM Controller**. The **Summit WM Controller** page is displayed.



System Log Level

Summit™ Controller Log Level: Information

Altitude™ AP Log Level: Major

Health Checking

□ Disable Poll Timer

Syslog

□ Syslog Server IP: Port#: 514

□ Syslog Server IP: Port#: 514

□ Syslog Server IP: Port#: 514

□ Include all service messages

□ Include audit messages

Facilities: Application Logs: local.0

Service Logs: local.3

Audit Logs: local.6

System Shutdown

● Halt system: reboot

○ Halt system: reset database to factory default and reboot

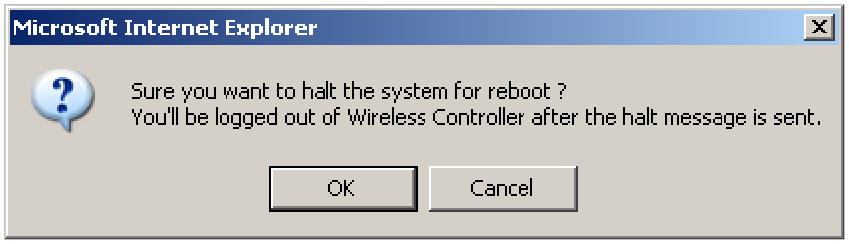
○ Halt system: reset to factory default and reboot

○ Halt system

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 04:14] User: admin Port status: M 1 2 3 4 F

3 Under **System Shutdown**, select **Halt System**, and then click **Apply Now**. The following dialogue box is displayed.



Sure you want to halt the system for reboot ?
You'll be logged out of Wireless Controller after the halt message is sent.

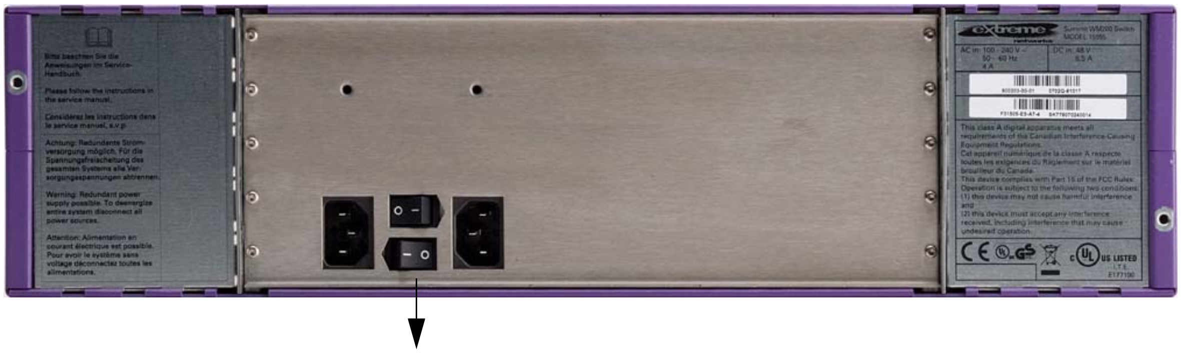
4 Click **OK**. The software's operations is halted and you are logged out of the system.

NOTE

An alternative method of stopping the software operation is to use the CLI commands. For more information, see the Summit WM CLI Reference Guide.

5 Switch off the Summit WM200/2000 Controller's power switches, located on the back panel. The Summit WM200/2000 Controller is now completely powered off.

Figure 20: Summit WM200/2000 Controller power switches



WARNING!

Do not power off the Summit WM200/2000 Controller by using the power switches only. Instead, carry out the entire procedure as described above. Failure to do so may corrupt the data on the hard disk drive.

Maintaining the Summit WM20 Controller

WARNING!

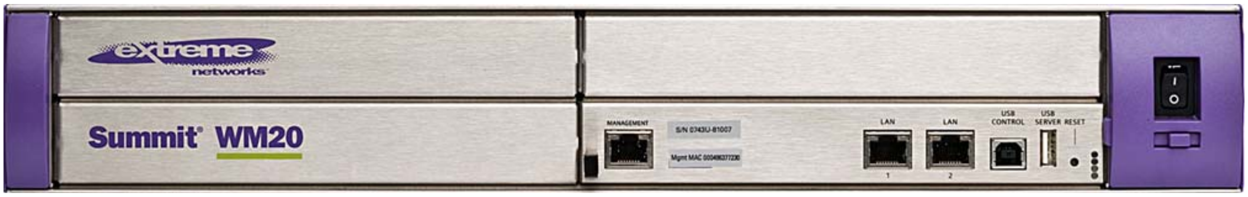
You should avoid operating the Summit WM20 in a LAN in which the DC voltage is overlaid on the data lines because the LAN may have switches that connect directly without checking the supply voltage. Depending upon the transformer at the LAN interface, voltages of up to 500 Volts can be induced. Such peak voltages can destroy the physical LAN controller's logic.

NOTE

The Summit WM20 can operate with either 110 or 230 V AC.

No electrical connection exists between the Altitude APs and the Summit WM20. The Summit WM20 and the Altitude APs communicate with each other via the IP network. For more information, see the *Summit WM User Guide*.

Figure 21: Summit WM20 Controller



NOTE

The USB Server Port is not used in the current release.

Summit WM20 Controller LEDs

The Summit WM20 Controller has four lights on its front panel. For more information, see the *Summit WM User Guide*.

Maintenance:

If a WM20 develops a problem, you should ship it to Extreme Networks.

WARNING!

Properly shut down the system before shipping the Summit WM20 Controller. The sequential steps to power off the Summit WM20 Controller are similar to powering off the Summit WM200/2000 Controller. For more information, see "Powering off the Summit WM200/2000 Controller" on page 120.

Backing up the Summit WM20 Controller system configuration:

You can backup the Summit WM20 Controller's system configuration. You can also define the automatic schedule backups to occur. While defining a scheduled backup, you can configure to have the backup copied to an FTP server. The backup will be copied to the FTP server after the backup is completed on the local drive. For more information, refer to the *Summit WM User Guide*.

WARNING!

Whenever you change the system configuration, you must always define the automatic schedule backup to be copied to the FTP server. If this not done, you may not able to retrieve the system configuration in the event of HDD failure.

Summit WM20 Controller power and maintenance procedures

The power and maintenance procedures for the Summit WM20 Controller is similar to the Summit WM200/2000 Controller. For more information, see "Powering off the Summit WM200/2000 Controller" on page 120.

11 Performing Altitude AP software maintenance

Periodically, the software used by the Altitude APs is altered for reasons of upgrade or security. The new version of the AP software is installed from the Summit WM Controller.

The software for each Altitude AP can be uploaded either immediately, or the next time the Altitude AP connects. Part of the Altitude AP boot sequence is to seek and install its software from the Summit WM Controller.

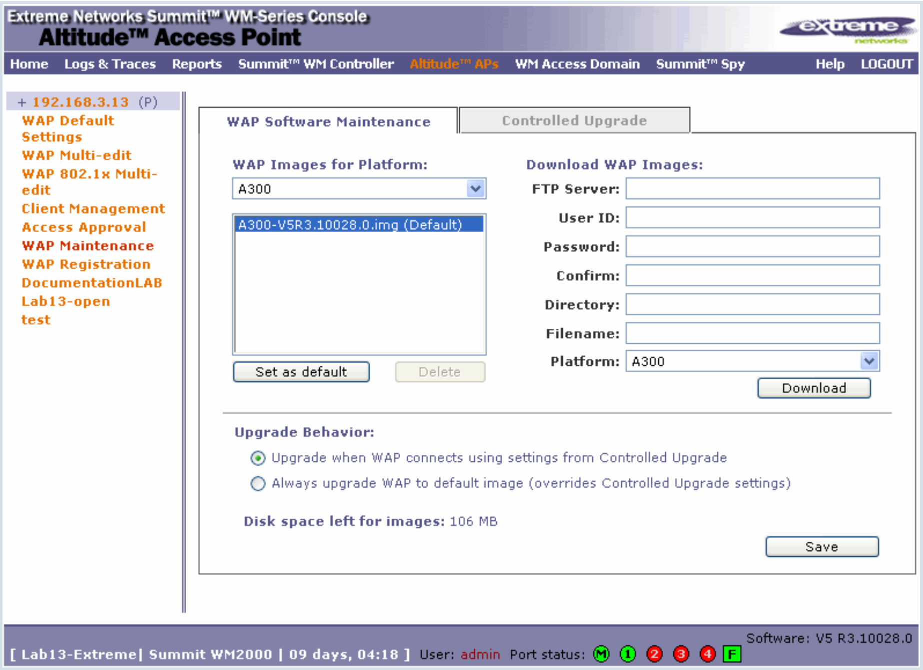
Most of the properties of each radio on a Altitude AP can be modified without requiring a reboot of the AP.

The Altitude AP keeps a backup copy of its software image. When a software upgrade is sent to the Altitude AP, the upgrade becomes the Altitude AP's current image and the previous image becomes the backup. In the event of failure of the current image, the Altitude AP will run the backup image.

To maintain the list of current Altitude AP software images:

1 From the main menu, click **Altitude APs**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.



WAP Images for Platform: A300

A300-V5R3.10028.0.img (Default)

Download WAP Images:

FTP Server:

User ID:

Password:

Confirm:

Directory:

Filename:

Platform: A300

Upgrade Behavior:

● Upgrade when WAP connects using settings from Controlled Upgrade

○ Always upgrade WAP to default image (overrides Controlled Upgrade settings)

Disk space left for images: 106 MB

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 04:18] User: admin Port status: M 1 2 3 4 F

3 In the **WAP Images for Platform** drop-down list, click the appropriate platform.

4 To select an image to be the default image for a software upgrade, click it in the list, and then click **Set as default**.

5 In the **Upgrade Behavior** section, select one of the following:

- **Upgrade when WAP connects using settings from Controlled Upgrade** – The **Controlled Upgrade** tab is displayed. Controlled upgrade allows you to individually select and control the state of an AP image upgrade: which APs to upgrade, when to upgrade, how to upgrade, and to which image the upgrade or downgrade should be done. Administrators decide on the levels of software releases that the equipment should be running.

- **Always upgrade WAP to default image (overrides Controlled Upgrade settings) –** Selected by default. Allows for the selection of a default revision level (firmware image) for all APs in the domain. As the AP registers with the controller, the firmware version is verified. If it does not match the same value as defined for the default-image, the AP is automatically requested to upgrade to the default-image.

6 To save your changes, click **Save**.

To delete a Altitude AP software image:

1 From the main menu, click **Altitude APs**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 In the **WAP Images for Platform** drop-down list, click the appropriate platform.

4 In the **WAP Images** list, click the image you want to delete.

5 Click **Delete**. The image is deleted.

To download a new Altitude AP software image:

1 From the main menu, click **Altitude APs**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 In the **Download WAP Images** list, type the following:

- **FTP Server –** The IP of the FTP server to retrieve the image file from.
- **User ID –** The user ID that the controller should use when it attempts to log in to the FTP server.
- **Password –** The corresponding password for the user ID.
- **Confirm –** The corresponding password for the user ID to confirm it was typed correctly.
- **Directory –** The directory on the server in which the image file that is to be retrieved is stored.
- **Filename –** The name of the image file to retrieve.
- **Platform –** The AP hardware type to which the image applies. The are several types of AP and they require different images.

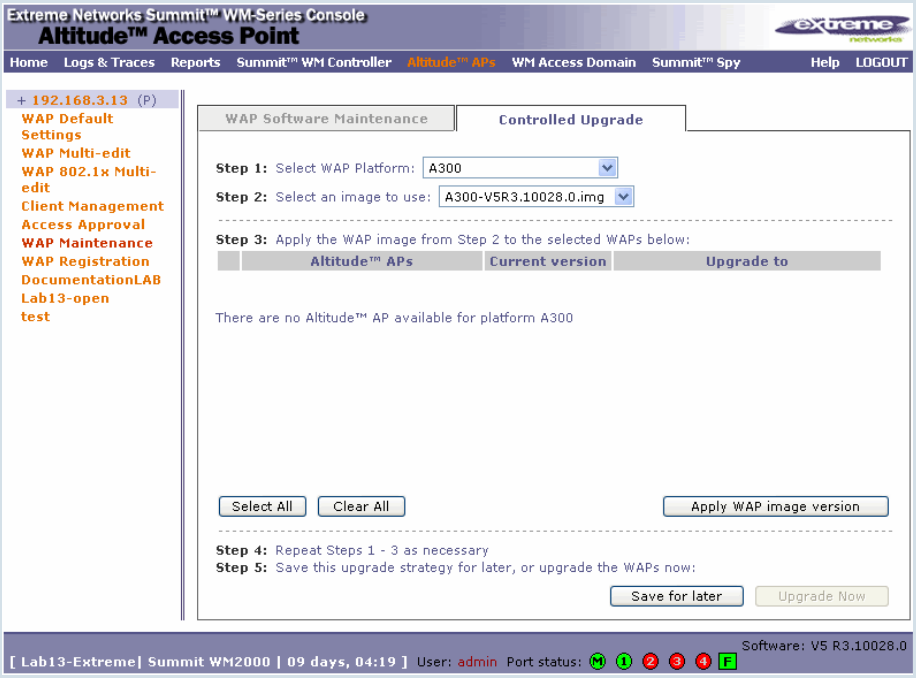
4 Click **Download**. The new software image is downloaded.

To define parameters for a Altitude AP controlled software upgrade:

1 From the main menu, click **Altitude APs**. The **Altitude APs** page is displayed.

2 From the left pane, click **WAP Maintenance**. The **WAP Software Maintenance** tab is displayed.

3 Click the **Controlled Upgrade** tab.



Step 1: Select WAP Platform: A300

Step 2: Select an image to use: A300-V5R3.10028.0.img

Step 3: Apply the WAP image from Step 2 to the selected WAPs below:

	Altitude™ APs	Current version	Upgrade to

There are no Altitude™ AP available for platform A300

Step 4: Repeat Steps 1 - 3 as necessary

Step 5: Save this upgrade strategy for later, or upgrade the WAPs now:

Software: V5 R3.10028.0

[Lab13-Extreme| Summit WM2000 | 09 days, 04:19] User: admin Port status: M 1 2 3 4 F

NOTE

*The **Controlled Upgrade** tab will appear only when the **Upgrade Behavior** is set to **Upgrade when AP connects using settings from Controlled Upgrade** on the **WAP Software Maintenance** tab.*

4 In the **Select WAP Platform** drop-down list, click the type of AP you want to upgrade.

5 In the **Select an image to use** drop-down list, click the software image you want to use for the upgrade.

6 In the list of registered **Altitude APs**, select the checkbox for each Altitude AP to be upgraded with the selected software image.

7 Click **Apply WAP image version**. The selected software image is displayed in the **Upgrade To** column of the list.

8 To save the software upgrade strategy to be run later, click **Save for later**.

9 To run the software upgrade immediately, click **Upgrade Now**. The selected Altitude AP reboots, and the new software version is loaded.

NOTE

*The **Always upgrade WAP to default image** checkbox on the **WAP Software Maintenance** tab overrides the **Controlled Upgrade** settings.*

Index